

EXHIBIT 1

FILED
2024 JAN 25 11:13 AM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 24-2-01791-7 SEA

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

NOAH SAEEDY, VISHAL SHAH, TINA
WILKINSON, and M.C., a minor, by and
through his natural parent and legal
guardian, Moses Chatmann III, individually,
and on behalf of all others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION, a
Washington Corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Noah Saeedy, Vishal Shah (collectively, the “California Plaintiffs”) and Tina Wilkinson and M.C., a minor, by and through his natural parent and legal guardian Moses Chatmann III, (“Washington Plaintiffs”) (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, by and through their undersigned counsel, allege the following upon information and belief, except as to those allegations concerning Plaintiffs, which they allege upon personal knowledge.

I. NATURE AND OVERVIEW OF THE ACTION

1. The Microsoft Edge browser (“Edge”) is a proprietary, cross-platform internet browser¹ created and marketed by Defendant Microsoft Corp. (“Microsoft” or “Defendant”). Like its predecessor Internet Explorer, Edge has proven to be widely popular with internet users both in the United States and abroad, taking up the third-largest market share of all internet browsers across desktops and all platforms. Versions 90, 92, 93 and earlier and later versions of Edge offer a default “non-private” browsing mode, as well as a “private” browsing mode through the use of an “inPrivate” window.

2. Unbeknownst to users, Defendant programmed Versions 90, 92, 93, and earlier and later versions of Edge to surreptitiously intercept, collect, and send to Defendant a wide range of private data relating to users’ internet browsing activities, internet searches, and online shopping behavior, including while in “private” browsing mode. As this private data is intercepted and collected, it is associated with unique user identifiers that Defendant assigns to users, and/or cookies—small text files containing unique data by which to identify a user’s device—that it installs on users’ devices. Upon intercepting and receiving the private user data, unique user identifiers, and cookies from Edge, Defendant then links or binds the private user data to individual users through the unique user identifiers and cookies.

3. Edge sends the intercepted and collected private user data and the unique user identifiers and cookies to several Microsoft-controlled servers, including those servers located at nav.smartscreen.microsoft.com (the “SmartScreen Server”) and at <https://www.bing.com/api/shopping/v1> (the “Bing Server”).

4. By associating the collected private data with the unique user identifiers and cookies, Defendant can and does determine individual users’ precise internet browsing activities and habits.

¹ The terms “internet browser” and “web browser” are used interchangeably throughout this Complaint.

1 Defendant thus utilized and configured Versions 90, 92, and 93, and earlier and later versions of the
2 Edge browser to intercept, collect, and process personally identifiable private data.

3 5. Defendant intercepts, collects, and sends users' keyword search terms, URLs, and
4 unique user identifiers and cookies to the SmartScreen and Bing servers without users' actual or
5 implied consent. Defendant fails to conspicuously present its flawed and deficient Privacy
6 Statement and Terms of Use to users and thus these electronic documents have no legal effect .

7 6. As such, Defendant's practices have and continue to result in numerous violations of
8 both federal and state laws as described herein.

9 II. PARTIES

10 **Plaintiff Noah Saeedy ("Plaintiff Saeedy" or "Saeedy")**

11 7. Plaintiff Saeedy resides in Glendora, California. Plaintiff Saeedy has used Edge since
12 at least June of 2021 (including, but not limited to, Versions 90, 92, and 93 of Edge) and used Edge
13 from his personal computer daily or weekly for both personal and work purposes. Plaintiff Saeedy
14 engaged in numerous sensitive financial activities using the Microsoft Edge browser, including
15 logging into his personal and business banking accounts, applying for a business loan, processing
16 business insurance claims, managing retirement and stock brokerage accounts, and viewing as well
17 as downloading his tax returns. Furthermore, Plaintiff Saeedy frequently utilized financial
18 management and credit monitoring services such as Credit Karma, Experian, Mint (which
19 transitioned to Intuit), and The Smarter Credit. Plaintiff Saeedy also used the Edge browser to shop
20 on Amazon and eBay's websites.

21 8. In addition to financial activities, Plaintiff Saeedy has used the Edge browser for
22 various medical-related inquiries and tasks, including research regarding health conditions,
23 medications, prices, and local pharmacies. His work necessitated him to access and handle patients'
24 health records and to research rules and regulations pertaining to workplace health standards using
25 the Edge browser.

1 9. Plaintiff Saeedy was frequently logged into his Microsoft account while using the
2 Edge browser, even when using Edge in “private” mode. While Saeedy used the Edge browser,
3 Microsoft Bing served as the default search engine, supplemented occasionally by Duck Duck Go.
4 Plaintiff Saeedy also regularly employed Google and Yahoo for a multitude of searches related to
5 work and personal matters, including “How To” guides, medical information, legal research, and
6 product searches. Additionally, he frequently conducted targeted searches within his email
7 accounts, utilizing search terms and filters for specific queries.

8 10. Plaintiff Saeedy has a reasonable expectation of privacy in his private data described
9 herein as well as in the collection and processing of his unique user identifiers in connection with
10 that data. Plaintiff Saeedy has property rights and interests in his private data described herein such
11 that the interception and use of that data is violative of those rights and therefore causes him injury
12 and damages. Plaintiff Saeedy would not have used the Edge browser had he known Defendant was
13 collecting, intercepting, and using his private data. Plaintiff Saeedy could not provide consent to
14 the interception and use because he did not know that his private content was being collected,
15 intercepted, and used by Defendant, and reasonably anticipated that his private data described herein
16 and associated unique user identifiers and cookies would remain private. Plaintiff Saeedy has
17 suffered further economic injury as a result of Defendant’s unlawful and unauthorized interceptions
18 and recordings of communications. Defendant used Plaintiff Saeedy’s private data for various
19 purposes, including, but not limited to, improving its software, services, and devices, providing
20 targeted advertising, and developing its sophisticated artificial intelligence and machine-learning
21 systems.

22 **Plaintiff Vishal Shah (“Plaintiff Shah” or “Shah”)**

23 11. Plaintiff Shah resides in Buena Park, California. Plaintiff Shah has used Edge since
24 at least June of 2021 (including, but not limited to, Versions 90, 92, and 93 of Edge) from a computer
25 provided by his employer and/or workplace. Plaintiff Shah engaged in numerous sensitive financial
26 activities using the Microsoft Edge browser, including logging into his banking accounts with Wells

1 Fargo and Chase, and actively managing his investments through platforms such as Weeble, Charles
2 Schwab, and Acorn. Furthermore, Plaintiff Shah utilized Credit Karma and Experian for credit
3 monitoring and financial management purposes. Plaintiff Shah also frequently used the Edge
4 browser to shop on Amazon and Best Buy's websites.

5 12. Moreover, Plaintiff Shah used the Edge browser for medical-related purposes,
6 including accessing his medical records through Kaiser's online portal and conducted searches on
7 how to treat a skin infection.

8 13. Plaintiff Shah was frequently logged into his Microsoft account while using the Edge
9 browser. In his interactions with the Edge browser, Microsoft Bing served as the default search
10 engine along with Google and Yahoo. Plaintiff Shah routinely conducted searches within his email
11 accounts, including Gmail and Yahoo, for both personal and professional communications. Despite
12 his expectation of privacy, particularly in instances where he used the Edge browser in "private"
13 mode, Plaintiff Shah experienced targeted advertising based on his activities and searches, including
14 those conducted in "private" mode.

15 14. Plaintiff Shah has a reasonable expectation of privacy in his private data described
16 herein as well as in the collection and processing of his unique user identifiers in connection with
17 that data. Plaintiff Shah has property rights and interests in his private data described herein such
18 that the interception and use of that data is violative of those rights and therefore causes him injury
19 and damages. Shah would not have used the Microsoft Edge browser had he known Defendant was
20 collecting, intercepting, and using his private data. Plaintiff Shah could not provide consent to the
21 interception and use because he did not know that his private content was being collected,
22 intercepted, and used by Defendant, and reasonably anticipated that his private data described herein
23 and associated unique user identifiers and cookies would remain private. Shah has suffered further
24 economic injury as a result of Defendant's unlawful and unauthorized interceptions and recordings
25 of communications. Defendant used Plaintiff Shah's private data for various purposes, including,
26

1 but not limited to, improving its software, services, and devices, providing targeted advertising, and
2 developing its sophisticated artificial intelligence and machine-learning systems.

3 **Plaintiff Tina Wilkinson (“Plaintiff Wilkinson” or “Wilkinson”)**

4 15. Plaintiff Wilkinson resides in Richland, Washington. Plaintiff Wilkinson has used
5 Edge since at least June of 2021 (including, but not limited to, Versions 90, 92, and 93 of Edge) on
6 a computer provided by an academic institution. Plaintiff Wilkinson used Edge to shop on third-
7 party websites.

8 16. In addition to using Edge for general shopping on third-party websites, Plaintiff
9 Wilkinson has extensively used the Edge browser for various financial and medical-related
10 activities. On the financial front, Plaintiff Wilkinson frequently logged into her personal banking
11 account and viewed her tax reports through the Edge browser. She has also used the Edge browser
12 to access and monitor her credit through Experian. Moreover, Plaintiff Wilkinson utilized Edge to
13 shop for a car, including using services like Carfax, and engaged in online shopping, during which
14 she entered her credit card information for purchases.

15 17. In terms of medical-related usage, Plaintiff Wilkinson used the Edge browser to
16 search for and access insurance information. She conducted private searches for her own medical
17 conditions she expected to be confidential and sought information on how to treat her skin infection.

18 18. Plaintiff Wilkinson was frequently logged into her Microsoft account while using the
19 Edge browser, even when using the browser in Private Mode. In his interactions with the Edge
20 browser. In her interactions with the Edge browser, she used the Google, Yahoo and Microsoft Bing
21 search engines. Despite her expectation of privacy, particularly in instances where she used the
22 Edge browser in “private” mode, Plaintiff Wilkinson experienced targeted advertising based on her
23 activities and searches, including those conducted in “private” mode.

24 19. Plaintiff Wilkinson has a reasonable expectation of privacy in her private data
25 described herein as well as in the collection and processing of her unique user identifiers in
26 connection with that data. Plaintiff Wilkinson has property rights and interests in her private data

described herein such that the interception and use of that data is violative of those rights and therefore causes her injury and damages. Plaintiff Wilkinson would not have used the Microsoft Edge browser had she known Defendant was collecting, intercepting, and using her private data. Plaintiff Wilkinson could not provide consent to the interception and use because she did not know that her private data was being collected, intercepted, and used by Defendant, and reasonably anticipated that her private data described herein and associated unique user identifiers and cookies would remain private. Plaintiff Wilkinson has suffered further economic injury as a result of Defendant's unlawful and unauthorized interceptions and recordings of communications. Defendant used Plaintiff Wilkinson's private data for various purposes, including, but not limited to, improving its software, services, and devices, providing targeted advertising, and developing its sophisticated artificial intelligence and machine-learning systems.

Plaintiff M.C., a minor, ("Plaintiff M.C." or "M.C.")

20. Plaintiff M.C. resides in Bremerton, Washington. Plaintiff M.C. has used Microsoft Edge since at least 2020 (including, but not limited to, Versions 90, 92, and 93 of Edge) from both his personal computer and a school-provided computer. Plaintiff M.C. is homeschooled, and thus uses the Edge browser for almost all of his educational tasks.

21. Additionally, Plaintiff M.C. uses the Edge browser for his specialized medical needs, researching about his autism spectrum condition, and attending online speech therapy and sensory courses. Plaintiff M.C. also frequently uses the browser for telehealth services, which often require him to input his sensitive financial information to pay for certain treatments, courses, and medication.

22. Plaintiff M.C. also used Edge to shop on Amazon's website and search on Google and Yahoo's search engine.

23. Plaintiff M.C. is almost always logged into his Microsoft account while using the Edge browser, even when using the browser in Private Mode. Despite his expectation of privacy, particularly in instances where he used the Edge browser in private mode, Plaintiff M.C. experienced

1 targeted advertising based on his activities and searches, including those conducted in private mode.
 2 These targeted advertisements have become so disruptive that Plaintiff M.C. is actively seeking ad
 3 blocker services.

4 24. Plaintiff M.C. has a reasonable expectation of privacy in his private data described
 5 herein as well as in the collection and processing of his unique user identifiers in connection with
 6 that data. Plaintiff M.C. has property rights and interests in his private data described herein such
 7 that the interception and use of that data is violative of those rights and therefore causes him injury
 8 and damages. Plaintiff M.C. would not have used the Microsoft Edge browser had he known
 9 Defendant was intercepting, collecting, and sharing his private data. Plaintiff M.C. could not
 10 provide consent to the interception and use because he is a minor and further because he did not
 11 know that his private data was being collected, intercepted, and used by Defendant, and reasonably
 12 anticipated that his private data described herein and associated unique user identifiers and cookies
 13 would remain private. M.C. has suffered further economic injury as a result of Defendant's unlawful
 14 and unauthorized interceptions and recordings of communications. Defendant used Plaintiff M.C.'s
 15 private data for various purposes, including, but not limited to, improving its software, services, and
 16 devices, providing targeted advertising, and developing its sophisticated artificial intelligence and
 17 machine-learning systems.

18 **Defendant Microsoft**

19 25. Defendant Microsoft is a publicly traded company incorporated under the laws of
 20 Washington with its principal executive offices located at One Microsoft Way, Redmond,
 21 Washington 98052. Microsoft offers computer hardware and software products for business and
 22 personal use, including the Edge internet browser. Microsoft describes Edge as its "fast and secure
 23 browser that helps protect [users'] data, with built-in shopping tools designed to save [users] time
 24 and money."²

25
 26 ² Microsoft Corporation, Annual Report (Form 10-K), at 5 (July 28, 2022).

III. JURISDICTION AND VENUE

26. The Court has jurisdiction of this matter pursuant to RCW 2.08.010.

27. Venue is proper in this forum under RCW 4.12.025 because Defend does business in King County and its principal place of business is located in King County.

IV. SUBSTANTIVE ALLEGATIONS

A. The Microsoft Edge Internet Browser

28. Microsoft Edge is a proprietary, cross-platform internet browser created and marketed by Defendant. Microsoft first released the Edge browser to the general public in July 2015 as the successor to Defendant's highly successful Internet Explorer web browser, which was at one time the most-widely used internet browser in the world. Since being released to the public, Edge has undergone various iterations and updates, beginning with the original Version 20 in July 2015 to Version 120 at the time of the filing of this Complaint.

29. Defendant Microsoft describes Edge as its "fast and secure browser that helps protect [users'] data, with built-in shopping tools designed to save [users] time and money."³ Through Edge, users can, among other things, browse the internet and its numerous websites, access their email and social media accounts, conduct keyword searches, engage in online shopping and other e-commerce, download files, and communicate with their friends, family, and business colleagues.

30. Since its release, Edge has been available to users via download through Microsoft's website or the online Microsoft Store. Microsoft releases new versions of Edge to the public for download through what it refers to as "channels," first releasing new versions through its development channels, such as the "Beta Channel," to a sample set of users before deploying them broadly to the public through the "Stable Channel."⁴

³ Microsoft Corporation, Annual Report (Form 10-K), at 5 (July 28, 2022).

⁴ See *Overview of the Microsoft Edge Channels*, Microsoft, <https://learn.microsoft.com/en-us/deployedge/microsoft-edge-channels#channel-overview> (last visited July 21, 2023).

31. Additionally, Defendant's Windows 10 operating system—which, like Edge, was released in July 2015—comes with Edge pre-installed, thereby ensuring that Edge appears on any new computer purchased with Windows 10 or any computer that has had its operating system upgraded to Windows 10 from a previous version.

32. Like its predecessor Internet Explorer, Edge has proven to be widely popular with internet users both in the United States and abroad. According to web analytics service Statcounter, in the United States, where there are an estimated 299 million internet users, Edge owned the third-largest market share of all internet browsers across desktops and all platforms (*i.e.*, desktops, tablets, and mobile devices) as of December 2023, with approximately 14.3%⁵ and 8.35%⁶ market share, respectively. Internationally, where there are an estimated 5.16 billion internet users,⁷ Statcounter calculates that as of December 2023, Edge represented the second-largest market share of all internet browsers across desktops and the third-largest market share of all internet browsers across all platforms, with 11.89%⁸ and 4.97%⁹ market share, respectively. Put simply, Edge is used by tens of millions of people in the United States and hundreds of millions of people around the world.

⁵ See *Desktop Browser Market Share United States of America Jan 2020–Dec 2023*, statcounter, <https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america#monthly-202001-202312> (last visited January 22, 2024).

⁶ See *Browser Market Share United States of America Jan 2020–Dec 2023*, statcounter, <https://gs.statcounter.com/browser-market-share/all/united-states-of-america#monthly-202001-202312> (last visited January 22, 2024).

⁷ See Ani Petrosyan, *Number of internet and social media users worldwide as of January 2023 (in billions)*, statista (Apr. 3, 2023), <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

⁸ See *Desktop Browser Market Share Worldwide Jan 2020–Dec 2023*, statcounter, <https://gs.statcounter.com/browser-market-share/desktop/worldwide#monthly-202001-202312> (last visited January 22, 2024).

⁹ See *Browser Market Share Worldwide Jan 2020–Dec 2023*, statcounter, <https://gs.statcounter.com/browser-market-share#monthly-202001-202312> (last visited January 22, 2024).

**B. Versions 90, 92, 93, and Earlier and Later Versions of Edge Offer “Private”
Browsing Windows**

33. Versions 90, 92, 93, and earlier and later versions of Edge offer a default “non-private” browsing mode, as well as a “private” browsing mode through the use of an “inPrivate” window. When users open Version 90, 92, 93, and earlier and later versions of the Edge browser, a “non-private” browsing window appears. Users can select to open and browse through an inPrivate window by selecting it from the Edge browser’s options. Defendant describes its inPrivate window to users as a more private way to browse the internet that, among other things, “deletes [users’] browsing information when [they] close all inPrivate windows” and “prevents Microsoft Bing searches from being associated with [users].” Defendant neither clearly nor expressly explains that browsing the internet through an inPrivate window does not prevent Edge from intercepting, collecting, and sending data associated with users’ internet activity, including users’ search terms on websites, visited webpages, and online shopping activities, as well as users’ associated unique user identifiers and cookies, to Defendant.

C. Versions 90, 92, 93 and Earlier and Later Versions of Edge Surreptitiously Intercept and Collect Private User Data and Send it to Defendant

34. Unbeknownst to users, Defendant programmed Versions 90, 92, 93, and earlier and later versions of Edge to surreptitiously intercept, collect, and send to Defendant a wide range of private data relating to users’ internet browsing activities, internet searches, and online shopping behavior. As this data is collected, it is associated with unique user identifiers that Defendant assigns to users, and/or cookies—small text files containing unique data by which to identify a user’s device—that it installs on users’ devices. These unique user identifiers and cookies include the user’s: (i) Microsoft Machine Unique Identifier (“MUID”); (ii) WLS Identifier (“WLS”); (iii) Windows Live ID (“WLID”); (iv) impressionId; and (v) X-Client-Data.

35. The MUID cookie is a unique user identifier used for advertising, site analytics, and other operational purposes, which links the user data it collects to a specific user and consists of an alphanumeric string.

36. The WLS is a unique user identifier assigned to a specific user that consists of an alphanumeric string. The WLS also includes a user's real name.

37. The WLID is a unique user identifier assigned to a specific user that consists of an alphanumeric string.

38. The impressionId is a unique user identifier assigned to a specific user that consists of an alphanumeric string.

39. X-Client-Data is a user identifier assigned to a specific user that consists of an alphanumeric string.

40. Edge also collects and sends to Microsoft identifying information about a user's web browser, which it collectively terms "User-Agent Data."

41. Edge sends the collected user data and the unique user identifiers and cookies to several Microsoft-controlled servers, including those servers located at nav.smartscreen.microsoft.com (the "SmartScreen Server") and at https://www.bing.com/api/shopping/v1 (the "Bing Server").

42. Upon receiving the private user data, unique user identifiers, and cookies from Edge, Defendant then links or binds the user data to individual users through the unique user identifiers and cookies.

1. Microsoft Uses the Private Data It Surreptitiously Intercepts and Collects from Users

43. More than just intercepting and collecting the private data described herein from users of the Edge Browser, Defendant uses that data for various purposes, including, but not limited to, improving its software, services, and devices, and providing targeted advertising.

44. Microsoft's surreptitious interception, collection and use of private user data has

become so rampant that even fellow tech giant Twitter has accused Microsoft of misusing Twitter's data, with Twitter CEO Elon Musk also accusing Microsoft and its partner OpenAI of illegally using Twitter data to develop sophisticated artificial intelligence systems such as ChatGPT.¹⁰ On information and belief, Microsoft is also using the intercepted private user data described herein to develop its sophisticated artificial intelligence and machine-learning systems.

45. Edge users are not aware, and Defendant does not adequately provide them with notice, that Defendant uses users' private data described herein for various purposes, including, but not limited to, improving its software, services, and devices, providing targeted advertising, and developing its sophisticated artificial intelligence and machine-learning systems.

D. Microsoft Edge Version 90

46. Microsoft Edge Version 90 ("Version 90") was released via the Beta Channel on or around March 16, 2021 and was released through the Stable Channel on or around April 15, 2021.¹¹ Unbeknownst to users, Version 90 surreptitiously collects, intercepts, and sends to the Bing Server a wide range of private data relating to users' internet browsing and online shopping activities, and links that data with unique user identifiers and cookies, without users' knowledge or consent. By linking users' unique user identifiers, cookies, and User Agent Data with the collected data regarding users' internet browsing and online shopping activities, Defendant is able to identify individual users and associate them with their internet activities. The intercepted data includes, as further described herein, search queries and visited webpages.

1. Version 90 "Binds" User Identifiers

47. When a user opens Version 90 of the Edge Browser and is either already logged in to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the user's

¹⁰ David Hamilton, *Twitter accuses Microsoft of misusing its data, foreshadowing a possible fight over AI*, AP News, <https://apnews.com/article/twitter-microsoft-ai-training-data-dispute-musk-nadella-292fd9de9cc2623003fd1ce44897c912>.

¹¹ See *Microsoft Edge release schedule*, Microsoft, <https://learn.microsoft.com/en-us/deployedge/microsoft-edge-release-schedule> (last visited June 17, 2023).

WLS and MUID together in the same data packet, “binding” them together for the remainder of the user’s web-browsing session.¹² By having Version 90 process these unique user identifiers and/or cookies at the beginning of the user’s web-browsing session, Defendant is able to link them with the user’s internet browsing and online shopping activities and identify individual users. Defendant’s ability to identify individual users is further enhanced by Version 90’s processing of User Agent Data as the user browses the internet. Furthermore, by having Version 90 bind the user’s MUID and WLS together at the beginning of the user’s internet-browsing session, Defendant is able to continuously associate the user with his internet activity even if the MUID changes throughout the session.

2. Search Queries in Integrated Search Bars

48. Many websites contain an integrated search bar that allows any visitor to search for information on the website using search terms, similar to using an internet search engine like Bing, Google, or Yahoo. When a user runs a search query on a website using the website’s integrated search bar, the website will often return a list of search results with links to the specific webpages on the website that contain the information the user is searching for. A user can navigate to those webpages by clicking on the links.

49. Unbeknownst to Version 90 users, when a Version 90 user utilizes the integrated search bar on many websites, Edge collects, intercepts, and sends to the Bing Server the search terms entered by the user.

50. Version 90 collects, intercepts, and sends this data to the Bing Server even when the user is utilizing an inPrivate window.

51. Version 90 also collects and processes unique user identifiers and/or cookies associated with the user as it collects, intercepts, and sends to the Bing Server the user’s search

¹² If a user opens an inPrivate window to browse the internet, Version 90 does not process the user’s WLS or MUID at the start of the user’s session. However, on information and belief, Version 90 process the user’s MUID later in the session as the user browses the internet.

queries. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 90 also collects and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's search queries, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the collected search queries to individual users through their unique user identifiers and/or cookies, revealing to Defendant users' identities and internet search activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he ran the search, Defendant can additionally utilize the user's WLS to link the user to his search queries and identify the user, even if the user's MUID changes throughout the session because Version 90 "binds" it together with the user's MUID at the start of the user's session. Defendant's ability to identify users is further enhanced by Version 90's processing of User Agent Data.

52. Defendant uses the above-described private data for various purposes discussed above.

53. Version 90 users, including Plaintiffs and Class members, are unaware that Version 90 is collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

3. Visited Webpages

54. As users browse the internet using Edge, they navigate between different webpages. Each webpage has a unique uniform resource locator, also known as a "URL," which serves as the webpage's address on the internet.

55. Unbeknownst to Version 90 users, for many websites, whenever a Version 90 user visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the Bing Server the full URL of each webpage a user visits. Version 90 collects, intercepts, and sends this data to the Bing Server even when the user is utilizing an inPrivate window.

56. Version 90 also collects and processes unique user identifiers and/or cookies

1 associated with the user as it collects, intercepts, and sends to the Bing Server the user's visited
 2 URLs. These include the user's MUID and impressionId whether or not the user is logged in to his
 3 Microsoft Account. Version 90 also collects and processes the user's User Agent Data as it collects,
 4 intercepts, and sends to Defendant the user's visited URLs, whether or not the user is logged in to
 5 his Microsoft Account. Defendant is able to link the visited URLs to individual users through their
 6 unique user identifiers and/or cookies, revealing users' identities and internet search activity to
 7 Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate window
 8 when he visited the URL, Defendant can additionally utilize the user's WLS to link the user to his
 9 visited URLs and identify the user, even if the user's MUID changes throughout the session because
 10 Version 90 "binds" it together with the user's MUID at the start of the user's session. Defendant's
 11 ability to identify users is further enhanced by Version 90's processing of User Agent Data.

12 57. Defendant uses the above-described private data for various purposes discussed
 13 above.

14 58. Version 90 users, including Plaintiffs and the Class, are unaware that Version 90 is
 15 collecting, intercepting, and sending to Defendant the above-described private data, and that
 16 Defendant uses that data, and have not provided their consent, whether implied or express, for
 17 Defendant to collect, intercept, receive, or use this data.

18 **E. Microsoft Edge Version 92**

19 59. Microsoft Edge Version 92 ("Version 92") was released via the Beta Channel on or
 20 around June 8, 2021, and was released through the Stable Channel on or around July 22, 2021.¹³
 21 Unbeknownst to users, Edge Version 92 surreptitiously collects, intercepts, and sends to the Bing
 22 Server and/or SmartScreen Server a wide range of data relating to users' internet browsing and
 23 online shopping activities, and links that data with unique user identifiers and cookies, without
 24 users' knowledge or consent. By linking users' unique user identifiers, cookies, and User Agent
 25

26 ¹³ See *Microsoft Edge release schedule*, *supra*, note 11.

1 Data with the collected data regarding users' internet browsing and online shopping activities,
2 Defendant can identify individual users and associate them with their internet activities. The
3 intercepted data includes, as further described herein, search queries and visited webpages.

4 **1. Version 92 "Binds" User Identifiers**

5 60. When a user opens Version 92 of the Edge Browser and is either already logged in
6 to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the user's
7 WLS, MUID, WLID, and X-Client Data together in the same data packet, "binding" them together
8 for the remainder of the user's web-browsing session. By having Version 92 process these unique
9 user identifiers and/or cookies at the beginning of the user's web-browsing session, Defendant is
10 able to link them with the user's internet browsing and online shopping activities and identify
11 individual users. Defendant's ability to identify individual users is further enhanced by Version
12 92's processing of User Agent Data as the user browses the internet. Furthermore, by having
13 Version 92 bind the user's MUID, WLS, WLID, and X-Client-Data together at the beginning of the
14 user's internet-browsing session, Defendant is able to continuously associate the user with his
15 internet activity even if some of those identifiers change throughout the session.

16 **2. Search Queries in Integrated Search Bars**

17 61. Many websites contain an integrated search bar that allows any visitor to search for
18 information on the website using search terms, similar to using an internet search engine like Bing,
19 Google, or Yahoo. When a user runs a search query on a website using the website's integrated
20 search bar, the website will often return a list of search results with links to the specific webpages
21 on the website that contain the information the user is searching for. A user can navigate to those
22 webpages by clicking on the links.

23 62. Unbeknownst to Version 92 users, when a Version 92 user utilizes the integrated
24 search bar on many websites, Edge collects, intercepts, and sends to the Bing Server the search
25 terms entered by the user. Edge collects, intercepts, and sends this data to the Bing Server even
26 when the user is utilizing an inPrivate window.

63. Version 92 also collects and processes unique user identifiers and/or cookies associated with the user together with the user's search queries. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's search queries, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the collected search queries to individual users through their unique user identifiers and cookies, revealing users' identity and internet search activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate window when he ran the search, Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to his search queries and identify the user, even if some of those identifiers change throughout the session because Version 92 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by Version 92's processing of User Agent Data.

64. Defendant uses the above-described private data for various purposes discussed above.

65. Edge Version 92 users, including Plaintiffs and Class members, are unaware that Version 92 is collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

3. Search Queries in Search Engines

66. Edge Version 92 contains an address bar through which users can navigate the internet. Users can use the address bar to navigate to a specific website or webpage by entering the webpage's URL into the address bar.

67. Alternatively, users can use the address bar to enter search terms similar to the way they would use a search engine like Google or Yahoo. Edge allows users to select from one of several search engines to process their searches and return results when the address bar is used in this way. Users can select their preferred search engine through Edge's "Settings" menu. By

1 default, Edge sets Bing as the search engine to process users' searches. However, users can select
 2 between the Bing, Google, Yahoo, and DuckDuckGo search engines to process searches they enter
 3 into the address bar.

4 68. When used to conduct a search, the address bar functions in two ways:

5 69. First, as a user types each character that makes up the key terms of his or her search,
 6 Edge displays in real-time a list of potentially relevant search suggestions based on a prediction of
 7 the user's search terms. A user may select one of the suggested searches by clicking on it. If a user
 8 does so, the user's selected search engine will run the suggested search, and Edge will navigate the
 9 user to a page displaying results for that search on the selected search engine's website. From there,
 10 the user may click on any of the displayed results and navigate to the specific webpage on which
 11 they appear.

12 70. Second, a user may choose to forgo selecting one of the suggested searches displayed
 13 under the address bar as he enters search terms, and instead run his own search query using search
 14 terms he enters. Like when a user chooses a suggested search, the user's selected search engine will
 15 run the user's search query, and Edge will navigate the user to a page displaying results for that
 16 search on the selected search engine's website. From there, a user may click on any of the displayed
 17 results and navigate to the specific webpage on which they appear.

18 71. Unbeknownst to Version 92 users not utilizing an inPrivate window, when a user
 19 sets his default search engine to Yahoo and runs a search through the Edge address bar, Edge
 20 collects, intercepts, and sends to Defendant the user's search queries. Specifically, Edge collects
 21 this data and sends it to the SmartScreen Server, thereby revealing to Defendant the user's internet
 22 search activity. The same occurs if a user navigates to Yahoo's website and enters a search through
 23 the search bar located there.

24 72. Defendant uses the above-described private data for various purposes discussed
 25 above.

26 73. Edge users, including Plaintiffs and Class members, are unaware Defendant is

collecting the above-described data, regardless of whether they have chosen Bing to process their searches queries in the Edge address bar, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

4. Visited Webpages

74. As users browse the internet using Edge, they navigate between different webpages. Each webpage has a URL which serves as the webpage's address on the internet.

75. Unbeknownst to Version 92 users, for many websites, whenever a Version 92 user visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the Bing Server the full URL of each webpage a user visits. Version 92 collects, intercepts, and sends this data to the Bing Server even when the user is utilizing an inPrivate window.

76. Version 92 also collects and processes unique user identifiers and/or cookies associated with the user as it collects, intercepts, and sends to the Bing Server the user's visited URLs. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's visited URLs, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the visited URLs to individual users through their unique user identifiers and/or cookies, revealing to Defendant users' identities and internet search activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he visited the URL, Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to his visited URLs and identify the user, even if some of those identifiers change throughout the session because Version 92 "binds" them with the user's MUID at the start of the user's session. Defendant's ability to identify users is further enhanced by Version 92's processing of User Agent Data.

77. Defendant uses the above-described private data for various purposes discussed above.

78. Version 92 users, including Plaintiffs and Class members, are unaware that Version 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

F. Microsoft Edge Version 93

79. Microsoft Edge Version 93 (“Version 93”) was released via the Beta Channel on or around August 3, 2021 and was released through the Stable Channel on or around September 2, 2021.¹⁴ Unbeknownst to users, Edge Version 93 surreptitiously collects, intercepts, and sends to the Bing Server a wide range of data relating to users’ internet browsing and online shopping activities, and links that data with unique user identifiers and cookies, without users’ knowledge or consent. By linking users’ unique user identifiers, cookies, and User Agent Data with the collected data regarding users’ internet browsing and online shopping activities, Defendant is able to identify individual users and associate them with their internet activities. The intercepted data includes, as further described herein, search queries and visited webpages.

1. Version 93 “Binds” User Identifiers

80. When a user opens Version 93 of the Edge Browser and is either already logged in to his Microsoft Account or logs in to his Microsoft Account, Edge collects and processes the user’s WLS, MUID, and WLID together in the same data packet, “binding” them together for the remainder of the user’s web-browsing session. By having Version 93 process these unique user identifiers and/or cookies at the beginning of the user’s web-browsing session, Defendant is able to link them with the user’s internet browsing and online shopping activities and identify individual users. Defendant’s ability to identify individual users is further enhanced by Version 93’s processing of User Agent Data as the user browses the internet. Furthermore, by having Version 93 bind the user’s MUID, WLS, and WLID together at the beginning of the user’s internet-browsing

¹⁴ See *Microsoft Edge release schedule*, *supra*, note 11.

1 session, Defendant is able to continuously associate the user with his internet activity even if some
2 of those identifiers change throughout the session.

3 **2. Search Queries in Integrated Search Bars**

4 81. Many websites contain an integrated search bar that allows any visitor to search for
5 information on the website using search terms, similar to using an internet search engine like Bing,
6 Google, or Yahoo. When a user runs a search query on a website using the website's integrated
7 search bar, the website will often return a list of search results with links to the specific webpages
8 on the website that contain the information the user is searching for. A user can navigate to those
9 webpages by clicking on the links.

10 82. Unbeknownst to Version 93 users, when a Version 93 user utilizes the integrated
11 search bar on many websites that appear, Edge collects, intercepts, and sends to the Bing Server the
12 search terms entered by the user. Edge collects, intercepts, and sends this data to the Bing Server
13 even when the user is utilizing an inPrivate window.

14 83. Version 93 also collects and processes unique user identifiers and/or cookies
15 associated with the user together with the user's search queries. These include the user's MUID and
16 impressionId whether or not the user is logged in to his Microsoft Account. Version 93 also collects
17 and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the user's
18 search queries, whether or not the user is logged in to his Microsoft Account. Defendant is able to
19 link the collected search queries to individual users through their unique user identifiers and cookies,
20 revealing to Defendant users' identity and internet search activity. If a user was logged in to his
21 Microsoft Account and not using an inPrivate window when he ran the search, Defendant can
22 additionally utilize the user's WLS and WLID to link the user to his search queries and identify the
23 user, even if the WLID changes throughout the session because Version 93 "binds" them together
24 with the user's MUID at the start of the user's session. Defendant's ability to identify users is
25 enhanced by Version 93's processing of User Agent Data.

26 84. Defendant uses the above-described private data for various purposes discussed

1 above.

2 85. Edge Version 93 users, including Plaintiffs and Class members, are unaware that
3 Version 93 is collecting, intercepting, and sending to Defendant the above-described private data,
4 and that Defendant uses that data, and have not provided their consent, whether implied or express,
5 for Defendant to collect, intercept, receive, or use this data.

6 **3. Visited Webpages**

7 86. As users browse the internet using Edge, they navigate between different webpages.
8 Each webpage has a unique URL which serves as the webpage's address on the internet.

9 87. Unbeknownst to Version 93 users, for many websites, whenever a Version 93 user
10 visits those websites or URLs within those websites, Edge collects, intercepts, and sends to the Bing
11 Server the full URL of each webpage a user visits. Version 93 collects, intercepts, and sends this
12 data to the Bing Server even when the user is utilizing an inPrivate window.

13 88. Version 93 also collects and processes unique user identifiers and/or cookies
14 associated with the user as it collects, intercepts, and sends to the Bing Server the user's visited
15 URLs. These include the user's MUID and impressionId whether or not the user is logged in to his
16 Microsoft Account. Version 93 also collects and processes the user's User Agent Data as it collects,
17 intercepts, and sends the user's visited URLs to Defendant, whether or not the user is logged in to
18 his Microsoft Account. Defendant can link the visited URLs to individual users through their unique
19 user identifiers and/or cookies, revealing to Defendant users' identities and internet search activity.
20 If a user was logged in to his Microsoft Account and not using an inPrivate window when he visited
21 the URL, Defendant can additionally utilize the user's WLS and WLID to link the user to his visited
22 URLs and identify the user, even if the WLID changes throughout the session because Version 93
23 "binds" them with the user's MUID at the start of the user's session. Defendant's ability to identify
24 users is further enhanced by Version 93's processing of User Agent Data.

25 89. Defendant uses the above-described private data for various purposes discussed
26 above.

90. Version 93 users, including Plaintiffs and Class members, are unaware that Version 93 is collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

G. Earlier and Later Versions of Edge

91. On information and belief, as with Edge Versions 90, 92, and 93, and unbeknownst to users, earlier and later versions of Edge surreptitiously intercept, collect, and send to the Bing Server and/or SmartScreen Server a wide range of data relating to users' internet browsing and online shopping activities, and link that data with unique user identifiers and cookies without users' knowledge or consent. On information and belief, this occurs whether or not the user is logged in to his Microsoft Account. By linking users' unique user identifiers, cookies, and User Agent Data with the collected data regarding users' internet browsing and online shopping activities, Defendant can identify individual users and associate them with their internet activities. The intercepted data includes at least some of the same categories of data as those collected by Versions 90, 92, and 93.

92. Defendant uses the above-described private data for various purposes discussed above.

93. Users of earlier and later versions of Edge, including Plaintiffs and Class members, are unaware that these versions are collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

H. Versions 90, 92, 93, and Earlier and Later Versions of Edge Surreptitiously Intercept and Collect Users' Online Shopping Data

94. Versions 90, 92, 93, and earlier and later versions of Edge each collect, intercept, and send to Defendant via the Bing and/or SmartScreen Servers a plethora of data related to users' online shopping habits on some of the world's largest retail websites, including those of Amazon, eBay, Walmart, and Best Buy. As described in further detail below, Defendant's surreptitious conduct

includes the interception and collection of the URLs users visit, the search terms they input, the contents of the product pages they view (*e.g.*, product reviews, product images), and the contents of their shopping carts. Defendant indiscriminately intercepts and collects, and sends this data to Microsoft, with no regard for the nature of the product a user browses or purchases, even those items for intimate use.

95. Edge collects, intercepts, and sends this data to the Bing and/or SmartScreen Servers, and links it with users' unique user identifiers and cookies, which allows Defendant to identify users and associate them with the specific items they browsed or purchased as well as with their online shopping habits more broadly. Edge users, including Plaintiffs and the Class, are unaware that Defendant is collecting this data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, or receive this data.

1. Amazon

96. Amazon.com, Inc. ("Amazon") is one of the world's largest online marketplaces and retailers, with over 300 million active customer accounts¹⁵ and net sales of \$514 billion in 2022¹⁶. Through Amazon's website, located at www.amazon.com (the "Amazon Website"), users are able to view, place in their online shopping carts, and purchase products or items from private sellers, other retailers, or Amazon directly.

97. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users' data, including data related to their online shopping habits, when they visit the Amazon Website.

a. Version 90

98. Unbeknownst to Version 90 users, when a Version 90 user browses the Amazon Website using Version 90 of Edge, Version 90 does each of the following:

¹⁵ See *Amazon Stats, Growth, Sales, and More*, Amazon, <https://sell.amazon.com/blog/amazon-stats> (last visited July 21, 2023).

¹⁶ See *Amazon.com Announces Fourth Quarter Results*, Amazon, <https://ir.aboutamazon.com/news-release/news-release-details/2023/Amazon.com-Announces-Fourth-Quarter-Results/default.aspx> (last visited July 21, 2023).

- 1 • **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms
2 entered by the user into the integrated search bar on the Amazon Website;
- 3 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
4 user navigates to, including the URL for the page of each product or item the user
5 clicks on and views. If a user navigated to the product by first running a search using
6 the Amazon Website’s integrated search bar, the user’s search terms are also included
7 among the data collected, intercepted, and sent to the Bing Server when the user
8 navigates to the product page;
- 9 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server, the
10 content of the reviews left by other users for each product or item the user clicks on
11 and views; and
- 12 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server, the
13 ratings left by other users for each product or item the user clicks on and views.

14 This data collection occurs even when the user is utilizing an inPrivate window.

15 99. Together with the above-described data, Version 90 also collects and processes
16 unique user identifiers and/or cookies associated with the user. These include the user’s MUID and
17 impressionId whether or not the user is logged in to his Microsoft Account. Version 90 also collects
18 and processes the user’s User Agent Data as it collects, intercepts, and sends to Defendant the above-
19 described data, whether or not the user is logged in to his Microsoft Account. Defendant is able to
20 link the above-described data to individual users through their unique user identifiers and/or cookies,
21 revealing to Defendant users’ identities and online shopping activity. If a user was logged in to his
22 Microsoft Account and not using an inPrivate window when he browsed the Amazon Website,
23 Defendant can additionally utilize the user’s WLS to link the user to the above-described data and
24 identify the user, even if the user’s MUID changes throughout the session because Version 90
25 “binds” it together with the user’s MUID at the start of the user’s session. Defendant’s ability to
26 identify users is further enhanced by Version 90’s processing of User Agent Data.

100. Defendant uses the above-described private data for various purposes discussed above.

101. Version 90 users, including Plaintiffs and Class members, are unaware that Version 90 is collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

b. Version 92

102. Unbeknownst to Version 92 users, when a Version 92 user browses the Amazon Website using Version 92 of Edge, Version 92 does each of the following:

- **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms entered by the user into the integrated search bar on the Amazon Website;
- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views. If a user navigated to the product by first running a search using the Amazon Website's integrated search bar, the user's search terms are also included among the data collected, intercepted, and sent to the Bing Server when the user navigates to the product page;
- **Shopping Cart Contents:** Intercepts and collects, and sends to the Bing Server, the title, price, quantity, and URL for each product or item in the user's shopping cart;
- **Product Reviews:** Scrapes and collects, and sends to the Bing Server, the content of the reviews left by other users for each product or item the user clicks on and views; and
- **Product Ratings:** Scrapes and collects, and sends to the Bing Server, the ratings left by other users for each product or item the user clicks on and views.

This data collection occurs even when the user is utilizing an inPrivate window.

103. Together with the above-described data, Version 92 also collects and processes unique user identifiers and/or cookies associated with the user. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the above-described data, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and cookies, revealing to Defendant users' identities and online shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the Amazon Website, Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user, even if some of those identifiers change throughout the session because Version 92 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by Version 92's processing of User Agent Data.

104. Defendant uses the above-described private data for various purposes discussed above.

105. Edge Version 92 users, including Plaintiffs and Class members, are unaware that Version 92 is collecting, intercepting, and sending to Defendant the above-described private data, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

c. Version 93

106. Unbeknownst to Version 93 users, when a Version 93 user browses the Amazon Website using Version 93 of Edge, Version 93 does each of the following:

- **URLs:** Collects, intercepts, and sends to the Bing Server, the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views;
- **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server, the

1 title, price, quantity, image (and URL for that image), and URL for each product or
 2 item in the user's shopping cart;

- 3 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server, the
 4 content of the reviews left by other users for each product or item the user clicks on
 5 and views;
- 6 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server, the
 7 ratings left by other users for each product or item the user clicks on and views; and
- 8 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
 9 image (and URL for that image) of each product or item the user clicks and views.

10 This data collection occurs even when the user is utilizing an inPrivate window.

11 107. Together with the above-described data, Version 93 also collects and processes
 12 unique user identifiers and/or cookies associated with the user. These include the user's MUID and
 13 impressionId whether or not the user is logged in to his Microsoft Account. Version 93 also collects
 14 and processes the user's User Agent Data as it collects, intercepts, and sends the above-described
 15 data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able
 16 to link the above-described data to individual users through their unique user identifiers and cookies,
 17 revealing to Defendant users' identities and online shopping activity. If a user was logged in to his
 18 Microsoft Account and not using an inPrivate window when he browsed the Amazon Website,
 19 Defendant can additionally utilize the user's WLS and WLID to link the user to the above-described
 20 data and identify the user, even if the WLID changes throughout the session because Version 93
 21 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability
 22 to identify users is enhanced by Version 93's processing of User Agent Data.

23 108. Defendant uses the above-described private data for various purposes discussed
 24 above.

25 109. Edge Version 93 users, including Plaintiffs and Class members, are unaware that
 26 Version 93 is collecting, intercepting, and sending the above-described private data to Defendant,

and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

2. eBay

110. eBay Inc. (“eBay”) is one of the world’s largest online marketplaces, with approximately 138 million active users in 2022 and revenue of nearly \$10 billion in that year.¹⁷ Through eBay’s website, located at www.ebay.com (the “eBay Website”), users are able to view, place in their online shopping carts, and purchase or bid on products or items from private sellers or retailers.

111. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users’ data, including data related to their online shopping habits, when they visit the eBay Website.

a. Version 92

112. Unbeknownst to Version 92 users, when a Version 92 user browses the eBay Website using Version 92 of Edge, Version 92 does each of the following:

- **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms entered by the user into the integrated search bar on the eBay Website. Furthermore, if a user is not logged in to his Microsoft Account, Version 92 also collects, intercepts, and sends the user’s search terms to the SmartScreen server;
- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views; and
- **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the image (and URL for that image) of each product or item the user clicks and views when a user is not utilizing an inPrivate window to browse the eBay website.

113. Together with the above-described data, Version 92 also collects and processes

¹⁷ *eBay Revenue and Usage Statistics (2023)*, Business of Apps, <https://www.businessofapps.com/data/ebay-statistics/> (last visited July 21, 2023).

unique user identifiers and/or cookies associated with the user. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects and processes the user's User Agent Data as it collects, intercepts, and sends to Defendant the above-described data, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and cookies, revealing users' identities and online shopping activity to Defendant. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the eBay Website, Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user, even if some of those identifiers change throughout the session because Version 92 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by Version 92's processing of User Agent Data.

114. Defendant uses the above-described private data for various purposes discussed above.

115. Edge Version 92 users, including Plaintiffs and Class members, are unaware that Version 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

b. Version 93

116. Unbeknownst to Version 93 users, when a Version 93 user browses the eBay Website using Version 93 of Edge, Version 93 does each of the following:

- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views;

- 1 • **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server the
- 2 content of the reviews left by other users for each product or item the user clicks on
- 3 and views;
- 4 • **Product Ratings:** Scrapes and collects, intercepts, and sends to the Bing Server the
- 5 ratings left by other users for each product or item the user clicks on and views; and
- 6 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
- 7 image (and URL for that image) of each product or item the user clicks and views
- 8 when a user is not utilizing an inPrivate window to browse the eBay website.

9 This data collection occurs even when the user is utilizing an inPrivate window.

10 117. Together with the above-described data, Version 93 also collects and processes
 11 unique user identifiers and/or cookies associated with the user. These include the user's MUID and
 12 impressionId whether or not the user is logged in to his Microsoft Account. Version 93 also collects
 13 and processes the user's User Agent Data as it collects, intercepts, and sends the above-described
 14 data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able
 15 to link the above-described data to individual users through their unique user identifiers and cookies,
 16 revealing to Defendant users' identities and online shopping activity. If a user was logged in to his
 17 Microsoft Account and not using an inPrivate window when he browsed the eBay Website,
 18 Defendant can additionally utilize the user's WLS and WLID to link the user to the above-described
 19 data and identify the user, even if the WLID changes throughout the session because Version 93
 20 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability
 21 to identify users is enhanced by Version 93's processing of User Agent Data.

22 118. Defendant uses the above-described private data for various purposes discussed
 23 above.

24 119. Edge Version 93 users, including Plaintiffs and Class members, are unaware that
 25 Version 93 is collecting, intercepting, and sending the above-described private data to Defendant,
 26 and that Defendant uses that data, and have not provided their consent, whether implied or express,

for Defendant to collect, intercept, receive, or use this data.

3. Best Buy

120. Best Buy Co., Inc. (“Best Buy”) is an American multinational consumer electronics retailer, with 1,144 retail stores worldwide in 2022.¹⁸ For its 2022 and 2023 fiscal years, Best Buy reported revenue of approximately \$51.8 billion and \$46.3 billion, respectively.¹⁹ Through Best Buy’s website, located at www.bestbuy.com (the “Best Buy Website”), users are able to view, place in their online shopping carts, and purchase products or items from Best Buy or “top-rated sellers.”²⁰

121. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users’ data, including data related to their online shopping habits, when they visit the Best Buy Website.

a. Version 90

122. Unbeknownst to Version 90 users, when a Version 90 user browses the Best Buy Website using Version 90 of Edge, Version 90 does each of the following:

- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views; and
- **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server the title, price, and description of each product a user clicks on as that information appears on that product’s webpage.

This data collection occurs even when the user is utilizing an inPrivate window.

123. Together with the above-described data, Version 90 also collects and processes

¹⁸ See *Best Buy Co., Inc., Continuing Operations—Number of Stores and Retail Square Footage*, Best Buy, https://s2.q4cdn.com/785564492/files/doc_earnings/2024/q1/earnings-result/Square-Footage-and-Store-Counts.pdf (last visited July 21, 2023).

¹⁹ See *Best Buy reports Q4 FY23 results*, Best Buy, <https://corporate.bestbuy.com/best-buy-reports-q4-fy23-results/> (last visited July 21, 2023).

²⁰ See *Partner Portal*, Best Buy, <https://partners.bestbuy.com/canada/marketplace> (last visited July 21, 2023).

unique user identifiers and/or cookies associated with the user. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 90 also collects and processes the user's User Agent Data as it collects, intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and/or cookies, revealing to Defendant users' identities and online shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the Best Buy Website, Defendant can additionally utilize the user's WLS to link the user to the above-described data and identify the user, even if the user's MUID changes throughout the session because Version 90 "binds" it together with the user's MUID at the start of the user's session. Defendant's ability to identify users is further enhanced by Version 90's processing of User Agent Data.

124. Defendant uses the above-described private data for various purposes discussed above.

125. Version 90 users, including Plaintiffs and Class members, are unaware that Version 90 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

b. Version 92

126. Unbeknownst to Version 92 users, when a Version 92 user browses the Best Buy Website using Version 92 of Edge, Version 92 does each of the following:

- **Search Terms:** When a user is logged in to his Microsoft Account, collects, intercepts, and sends to the Bing Server the search terms entered by the user into the integrated search bar on the Best Buy Website regardless of whether a user is utilizing an inPrivate window;
- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user

clicks on and views;

- **Shopping Cart Contents:** Scrapes, collects, intercepts, and sends to the Bing Server the URL and price of each product or item in the user's shopping cart when a user is utilizing an inPrivate window to browse the Best Buy website;
- **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the image (and URL for that image) of each product or item the user clicks and views when a user is not utilizing an inPrivate window to browse the Best Buy website; and
- **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server the title and price of each product a user clicks on as that information appears on that product's webpage when a user is not utilizing an inPrivate window to browse the Best Buy website.

127. Together with the above-described data, Version 92 also collects and processes unique user identifiers and/or cookies associated with the user. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects and processes the user's User Agent Data as it collects, intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and cookies, revealing to Defendant users' identities and online shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the Best Buy Website, Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to the above-described data and identify the user, even if some of those identifiers change throughout the session because Version 92 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by Version 92's processing of User Agent Data.

128. Defendant uses the above-described private data for various purposes discussed above.

129. Edge Version 92 users, including Plaintiffs and Class members, are unaware that Version 92 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

c. Version 93

130. Unbeknownst to Version 93 users, when a Version 93 user browses the Best Buy Website using Version 93 of Edge, Version 93 does each of the following:

- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views;
- **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the title, price, quantity, image URL (and therefore the ability to view the image), and URL for each product or item in the user's shopping cart;
- **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the image (and URL for that image) of each product or item the user clicks and views; and
- **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server the price and description of each product a user clicks on as that information appears on that product's webpage.

This data collection occurs even when the user is utilizing an inPrivate window.

131. Together with the above-described data, Version 93 also collects and processes unique user identifiers and/or cookies associated with the user. These include the user's MUID and impressionId whether or not the user is logged in to his Microsoft Account. Version 93 also collects and processes the user's User Agent Data as it collects, intercepts, and sends the above-described data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able to link the above-described data to individual users through their unique user identifiers and cookies,

revealing to Defendant users' identities and online shopping activity. If a user was logged in to his Microsoft Account and not using an inPrivate window when he browsed the Best Buy Website, Defendant can additionally utilize the user's WLS and WLID to link the user to the above-described data and identify the user, even if the WLID changes throughout the session because Version 93 "binds" them together with the user's MUID at the start of the user's session. Defendant's ability to identify users is enhanced by Version 93's processing of User Agent Data.

132. Defendant uses the above-described private data for various purposes discussed above.

133. Edge Version 93 users, including Plaintiffs and Class members, are unaware that Version 93 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant uses that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

4. Walmart

134. Walmart Inc. ("Walmart") is an American multinational retail corporation operating more than 10,500 stores throughout the world.²¹ For its 2023 fiscal year, Walmart reported revenue of \$611.3 billion.²² Through Walmart's website, located at www.walmart.com (the "Walmart Website"), users are able to view, place in their online shopping carts, and purchase products or items from Walmart or other sellers.²³

135. Unbeknownst to users, Edge intercepts and collects, and sends to Defendant, users' data, including data related to their online shopping habits, when they visit the Walmart Website.

²¹ See *Location Facts*, Walmart, <https://corporate.walmart.com/about/location-facts> (last visited July 21, 2023).

²² See *Walmart Releases Q4 and FY23 Earnings*, Walmart, <https://corporate.walmart.com/newsroom/2023/02/21/walmart-releases-q4-and-fy23-earnings> (last visited July 21, 2023).

²³ See *Walmart Marketplace*, Walmart, <https://marketplace.walmart.com/> (last visited July 21, 2023).

1 **a. Version 90**

2 136. Unbeknownst to Version 90 users, when a Version 90 user browses the Walmart
3 Website using Version 90 of Edge, Version 90 does each of the following:

- 4 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
5 user navigates to, including the URL for the page of each product or item the user
6 clicks on and views;
- 7 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
8 image (and URL for that image) of each product or item the user clicks and views;
9 and
- 10 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
11 the title and price of each product a user clicks on as that information appears on that
12 product's webpage.

13 137. Together with the above-described data, Version 90 also collects and processes
14 unique user identifiers and/or cookies associated with the user. These include the user's MUID and
15 impressionId whether or not the user is logged in to his Microsoft Account. Version 90 also collects
16 and processes the user's User Agent Data as it collects, intercepts, and sends the above-described
17 data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able
18 to link the above-described data to individual users through their unique user identifiers and/or
19 cookies, revealing to Defendant users' identities and online shopping activity. If a user was logged
20 in to his Microsoft Account and not using an inPrivate window when he browsed the Walmart
21 Website, Defendant can additionally utilize the user's WLS to link the user to the above-described
22 data and identify the user, even if the user's MUID changes throughout the session because Version
23 90 "binds" it together with the user's MUID at the start of the user's session. Defendant's ability to
24 identify users is further enhanced by Version 90's processing of User Agent Data.

25 138. Defendant uses the above-described private data for various purposes discussed
26 above.

139. Version 90 users, including Plaintiffs and Class members, are unaware that Version 90 is collecting, intercepting, and sending the above-described private data to Defendant, and that Defendant is using that data, and have not provided their consent, whether implied or express, for Defendant to collect, intercept, receive, or use this data.

b. Version 92

140. Unbeknownst to Version 92 users, when a Version 92 user browses the Walmart Website using Version 92 of Edge, Version 92 does each of the following:

- **Search Terms:** Collects, intercepts, and sends to the Bing Server the search terms entered by the user into the integrated search bar on the Walmart Website if a user is utilizing an inPrivate window;
- **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the user navigates to, including the URL for the page of each product or item the user clicks on and views;
- **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the title, price, and quantity for each product or item in the user's shopping cart when a user is not utilizing an inPrivate to browse the Walmart website. When a user is utilizing an inPrivate window, Version 92 scrapes, collects, intercepts, and sends to the Bing Server the price of the products in the user's shopping cart;
- **Product Reviews:** Scrapes and collects, intercepts, and sends to the Bing Server the content of the reviews left by other users for each product or item the user clicks on and views when a user is not utilizing an inPrivate to browse the Walmart website;
- **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the image (and URL for that image) of each product or item the user clicks and views when a user is not utilizing an inPrivate to browse the Walmart website; and
- **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server the title, price, and description of each product a user clicks on as that information

1 appears on that product's webpage when a user is not utilizing an inPrivate window
2 to browse the Walmart website.

3 141. Together with the above-described data, Version 92 also collects and processes
4 unique user identifiers and/or cookies associated with the user. These include the user's MUID and
5 impressionId whether or not the user is logged in to his Microsoft Account. Version 92 also collects
6 and processes the user's User Agent Data as it collects, intercepts, and sends the above-described
7 data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able
8 to link the above-described data to individual users through their unique user identifiers and cookies,
9 revealing users' identities and online shopping activity to Defendant. If a user was logged in to his
10 Microsoft Account and not using an inPrivate window when he browsed the Walmart Website,
11 Defendant can additionally utilize the user's WLS, WLID, and X-Client-Data to link the user to the
12 above-described data and identify the user, even if some of those identifiers change throughout the
13 session because Version 92 "binds" them together with the user's MUID at the start of the user's
14 session. Defendant's ability to identify users is enhanced by Version 92's processing of User Agent
15 Data.

16 142. Defendant uses the above-described private data for various purposes discussed
17 above.

18 143. Edge Version 92 users, including Plaintiffs and Class members, are unaware that
19 Version 92 is collecting, intercepting, and sending the above-described private data to Defendant,
20 and that Defendant uses that data, and have not provided their consent, whether implied or express,
21 for Defendant to collect, intercept, receive, or use this data.

22 **c. Version 93**

23 144. Unbeknownst to Version 93 users, when a Version 93 user browses the Walmart
24 Website using Version 93 of Edge, Version 93 does each of the following:
25
26

- 1 • **URLs:** Collects, intercepts, and sends to the Bing Server the URL of each page the
2 user navigates to, including the URL for the page of each product or item the user
3 clicks on and views;
- 4 • **Shopping Cart Contents:** Collects, intercepts, and sends to the Bing Server the title,
5 price, quantity, image URL (and therefore the ability to view the image), and URL
6 for each product or item in the user's shopping cart;
- 7 • **Product Images:** Scrapes and collects, intercepts, and sends to the Bing Server the
8 image URL (and therefore the ability to view the image) of each product or item the
9 user clicks and views. If the user is not utilizing an inPrivate window, Version 93
10 also scrapes, collects, intercepts, and sends to the Bing Server the image of each
11 product or item the user clicks and views; and
- 12 • **Product Page Contents:** Scrapes, collects, intercepts, and sends to the Bing Server
13 the price and description of each product a user clicks on as that information appears
14 on that product's webpage.

15 With the exception noted above relating to product or item images, this data collection occurs even
16 when the user is utilizing an in Private window.

17 145. Together with the above-described data, Version 93 also collects and processes
18 unique user identifiers and/or cookies associated with the user. These include the user's MUID and
19 impressionId whether or not the user is logged in to his Microsoft Account. Version 93 also collects
20 and processes the user's User Agent Data as it collects, intercepts, and sends the above-described
21 data to Defendant, whether or not the user is logged in to his Microsoft Account. Defendant is able
22 to link the above-described data to individual users through their unique user identifiers and cookies,
23 revealing users' identities and online shopping activity to Defendant. If a user was logged in to his
24 Microsoft Account and not using an inPrivate window when he browsed the Walmart Website,
25 Defendant can additionally utilize the user's WLS and WLID to link the user to the above-described
26 data and identify the user, even if the WLID changes throughout the session because Version 93

1 “binds” them together with the user’s MUID at the start of the user’s session. Defendant’s ability
2 to identify users is enhanced by Version 93’s processing of User Agent Data.

3 146. Defendant uses the above-described private data for various purposes discussed
4 above.

5 147. Edge Version 93 users, including Plaintiffs and Class members, are unaware that
6 Version 93 is collecting, intercepting, and sending the above-described private data to Defendant,
7 and that Defendant uses that data, and have not provided their consent, whether implied or express,
8 for Defendant to collect, intercept, receive, or use this data.

9 **5. Earlier and Later Versions of Edge**

10 148. On information and belief, as with Versions 90, 92, and 93, and unbeknownst to
11 users, when users of earlier and later versions of Edge browse the Amazon, eBay, Best Buy, and
12 Walmart Websites, those versions of the Edge Browser collect, intercept, and send to the Bing
13 Server and/or SmartScreen Server a wide range of data relating to users’ online shopping habits on
14 those websites and link that data with unique user identifiers and cookies (including MUID and X-
15 Client-Data) without users’ knowledge or consent. On information and belief, this occurs whether
16 or not the user is logged in to his Microsoft Account. By linking users’ unique user identifiers,
17 cookies, and User Agent Data with the collected data regarding users’ online shopping activities,
18 Defendant is able to identify individual users and associate them with the specific items they
19 browsed or purchased as well as with their online shopping habits more broadly. The intercepted
20 data includes at least some of the same categories of data as those collected by Versions 90, 92, and
21 93.

22 149. Defendant uses the above-described private data for various purposes discussed
23 above.

24 150. Users of earlier and later versions of Edge, including Plaintiffs and Class members,
25 are unaware that those versions are collecting, intercepting, and sending the above-described private
26 data to Defendant, and that Defendant uses that data, and have not provided their consent, whether

1 implied or express, for Defendant to collect, intercept, receive, or use this data.

2 **I. Microsoft Does Not Disclose Edge’s Data Collection Practices to Users, and Users Are**
3 **Not Given Adequate Legal Notice of Microsoft’s Privacy Policy**

4 151. Many Microsoft Edge users have the Edge browser embedded into their computer
5 because it came that way: pre-installed within the Windows Operating System. Quintessential
6 examples include: a college or law student who buys a laptop at her school bookstore with *Office*
7 *Home & Student* preinstalled; a white-collar worker given a company-owned laptop by her employer
8 with, for example, *Microsoft Office* preinstalled; government employees who operate Microsoft
9 products paid for by United States’ taxpayers. These illustrative examples are a tiny subset of the
10 massive swath of Microsoft’s user base who are not presented with *any* separate notice relating to
11 Microsoft Edge’s highly intrusive data collection practices.

12 152. Nor would any user of Edge who borrows a device, *e.g.*, a sibling or a roommate of
13 the device owner, be presented with any disclosure or link to any Microsoft policy or agreement.
14 Such users are given no notice of Microsoft’s Privacy Policy.

15 153. While many Edge users have Edge forced upon them—embedded as the default
16 browser within a larger package of software that they actually need (like Microsoft Word), a far
17 smaller number of users actually seek Edge out and download the software on its own. As of 2023,
18 for those standalone Edge users, the Privacy Statement that purportedly goes along with it is not
19 conspicuously, immediately or directly presented. Instead, the user must search for it, and then
20 press a separate link to access it. *See* Image 1, below.

Image 1:

Download Microsoft Edge

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EDGE

After installation, these terms are also viewable in Microsoft Edge at <edge://terms>.

These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to this software published by Microsoft and any software updates ("Software") (except to the extent such Software or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated Software). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY DOWNLOADING OR USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE SOFTWARE.

[Privacy statement](#)

Choose installation language

English (US)

Accept and download

154. Also, during the Edge download process, users are presented with a window that shows only the beginning of Microsoft's Software License Terms. See Image 1.

155. Users need not scroll through the full Software License Terms to download Edge, however. In fact, users need not scroll through the Software License Terms or press the link to the Privacy Statement: they can just download Edge by clicking the blue button depicted below without scrolling through or clicking on anything. See Image 2.

Image 2:

Download Microsoft Edge

limitation or exclusion may not apply to you because your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Source code for portions of Microsoft Edge is available free of charge from <https://thirdpartysource.microsoft.com> under the third party open source license terms provided at <https://aka.ms/thirdparty notices> and in Microsoft Edge at edge://credits after installation. Or to obtain this source code you may send a check or money order for US \$5.00, including the Edge version number, to:

Source Code Compliance Team
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Privacy statement

Choose installation language

English (US)

Accept and download

156. Upon information and belief, previous versions of Microsoft's Privacy Statement were presented in an even less conspicuous manner and did not provide adequate legal notice to users about Edge's data collection practices. Upon information and belief, previous versions of the Software License Terms also were presented in an even less conspicuous manner.

157. Edge users who did not personally or individually download Edge, as well as Edge users who are minors are similarly not provided adequate legal notice regarding Defendant's data collection practices in relation to the users' use of the Edge browser.

J. Plaintiffs and the Class's Personal Information Has Value

158. The value of personal data is well understood and generally accepted as a form of currency.

159. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

1 160. The robust market for user data has been analogized to the “oil” of the tech industry.²⁴
 2 A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows
 3 companies to acquire or maintain a competitive edge.”²⁵ That article noted that the value of a single
 4 Internet user—or really, a single user’s data—varied from about \$15 to more than \$40.

5 161. The Organization for Economic Cooperation and Development (“OECD”) itself has
 6 published numerous volumes discussing how to value data such as that which is the subject matter
 7 of this Complaint, including as early as 2013, with its publication “Exploring the Economic of
 8 Personal Data: A Survey of Methodologies for Measuring Monetary Value.”²⁶ The OECD
 9 recognizes that data is a key competitive input not only in the digital economy but in all markets:
 10 “Big data now represents a core economic asset that can create significant competitive advantage
 11 for firms and drive innovation and growth.”²⁷

12 162. In *The Age of Surveillance Capitalism*, Harvard Business School Professor
 13 Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed
 14 their business models from fee-for-services-provided to monetizing their users’ data—including
 15 user data that is not necessary for product or service use, which she refers to as “behavioral
 16 surplus.”²⁸ In essence, Professor Zuboff explains that revenue from user Internet data pervades
 17 every economic transaction in the modern economy. It is a fundamental assumption of these

18
 19 ²⁴ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017).
 20 <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

21 ²⁵ Pauline Glickman and Nicolas Glady, *What’s the Value of Your Data?* TechCrunch (Oct. 13,
 22 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>.

23 ²⁶ *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring
 24 Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013),
 25 <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

26 ²⁷ *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct.
 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

²⁸ SHOSHANNA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 166 (2019).

1 revenues that there is a **market** for this data; data generated by Internet users using Versions 90, 92,
2 93, and earlier and later versions of the Edge Browser has economic value.

3 163. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes:

4 Personal information is an important currency in the new millennium. The
5 monetary value of personal data is large and still growing, and corporate
6 America is moving quickly to profit from the trend. Companies view this
information as a corporate asset and have invested heavily in software that
facilitates the collection of consumer information.²⁹

7 164. This economic value has been leveraged largely by corporations who pioneered the
8 methods of its extraction, analysis, and use. However, the data also has economic value to Internet
9 users. Market exchanges have sprung up where individual users like Plaintiffs can sell or monetize
10 their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.³⁰
11 Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.³¹

12 165. There are countless examples of this kind of market, which is growing more robust
13 as information asymmetries are diminished when users discover how their data is being covertly
14 intercepted, collected, and used.

15 166. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article “The
16 Economics of Privacy,” published in the *Journal of Economic Literature*:

17 Such vast amounts of collected data have obvious and substantial
18 economic value. Individuals’ traits and attributes (such as a person’s age,
19 address, gender, income, preferences, and reservation prices, but also her
clickthroughs, comments posted online, photos uploaded to social media,
and so forth) are increasingly regarded as business assets that can be used

22 ²⁹ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056–57
23 (2004).

24 ³⁰ Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10,
2020), <https://wallethacks.com/apps-for-selling-your-data/>.

25 ³¹ Jacob Kastrenakes, *A New TikTok Clone hit the top of the App Store by Paying users to watch*
26 *videos*, The Verge (May 29, 2020), <https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival>.

to target services or offers, provide relevant advertising, or be traded with other parties.³²

167. There is also a private market for users' personal information. While there is a wide range in values, the prices are nonetheless significant. For example:

- “Each piece of personal info has a price tag. A Social Security number may sell for as little as \$1. Credit card, debit card and banking info can go for as much as \$110. Usernames and passwords for non-financial institution logins are \$1, but it can range from \$20 to \$200 for login info for online payment platforms.”³³
- “Researchers pored through the prices of personal data and information—called ‘fullz’ by those searching for ‘full credentials’—that are available for sale on nearly 50 different Dark Web marketplaces, finding that Japan, the UAE, and EU countries have the most expensive identities available at an average price of \$25.”³⁴
- “According to Comparitech, who researched the prices of stolen credit cards, hacked PayPal accounts, and private Social Security numbers on more than 40 different dark web marketplaces, the average price of each U.S. citizen’s “fullz,” or complete information including name, date of birth, address, phone number, account numbers and other information is \$8.”³⁵

³² Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. OF ECON. LITERATURE 2, 444 (June 2016), <https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf>.

³³ *Understanding the Illegal Market for Personal Information*, OnPoint Community Credit Union, <https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/#:~:text=Each%20piece%20of%20personal%20info,info%20for%20online%20payment%20platforms>.

³⁴ Jonathan Greig, *How much is your info worth on the Dark Web? For Americans, it's just \$8*, TechRepublic, <https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/>.

³⁵ *There's Value in Everything: Stop Underestimating the Value of Your Data on the Black Market*, Virtually Managed IT Solutions LLC, <https://vmits.com/theres-value-in-everything-stop-underestimating-the-value-of-your-data-on-the-black-market/>.

1 168. These rates are assumed to be discounted because they do not operate in competitive
2 markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users
3 can sell their own.

4 169. In short, there is a quantifiable economic value to Internet users' data that is greater
5 than zero. The exact number will be a matter for experts to determine.

6 **K. Plaintiffs and Class and Subclass Members Suffered an Economic Injury**

7 170. Property is the right of any person to possess, use, enjoy, or dispose of a thing,
8 including intangible things such as data or communications.

9 171. California courts have recognized the lost "property value" of personal information.
10 Recent changes in California law have also confirmed that individuals have a property interest in
11 their information. In 2018, California enacted the California Consumer Privacy Act ("CCPA").
12 Among other things, the CCPA permits businesses to purchase consumer information from
13 consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and
14 appraise – *i.e.*, to place a monetary value on – consumer data (Cal. Civ. Code § 1798.125(a)(2)).

15 172. Accordingly, Plaintiffs' and Class and Subclass members' private data described
16 herein is property under California law.

17 173. Defendant's interception, collection, and use of Plaintiffs' and Class and Subclass
18 members' private data described herein without authorization is a taking of Plaintiffs' and Class and
19 Subclass members' property. Plaintiffs and Class and Subclass members have a right to
20 disgorgement and/or restitution damages for the value of the improperly collected private data
21 described herein by Defendant through Versions 90, 92, 93, and earlier and later versions of the
22 Edge browser.

23 174. Plaintiffs and Class and Subclass members have suffered benefit of the bargain
24 damages, in that Defendant took more data than authorized. Those benefit of the bargain damages
25 also include, but are not limited to (i) loss of the promised benefits of their experience using Versions
26 90, 92, 93, and earlier and later versions of the Edge browser to browse the internet; (ii) loss of the

1 promised benefits of their experience on the websites they visited using Versions 90, 92, 93, and
2 earlier and later versions of the Edge browser from which those versions of the Edge Browser
3 collected their private data; (ii) out-of-pocket costs; and (iii) loss of control over property which has
4 marketable value.

5 175. To preserve their privacy, Plaintiffs and Class and Subclass members who now
6 understand at least some of Defendant's violations are presented with the choice of (i) reducing or
7 ending their use of Versions 90, 92, 93, and earlier and later versions of the Edge browser; or (ii)
8 knowingly accepting less privacy than they were promised. Each of these options deprives Plaintiffs
9 and Class and Subclass members of the benefits of their original bargain. There is no option that
10 recovers the property improperly intercepted and collected by Defendant.

11 176. Further, Plaintiffs and Class and Subclass members were denied the benefit of
12 knowing that Defendant was intercepting and collecting their private data described herein. Thus,
13 they were unable to mitigate the harms they incurred because of Defendant's actions. That is,
14 Defendant's lack of transparency prevented and still prevents Plaintiffs' and Class and Subclass
15 members' ability to mitigate the harms.

16 177. Defendant avoided costs they should have incurred because of its actions—had it
17 transparently disclosed its actions, it would have suffered losses stemming from the loss of user
18 engagement with Versions 90, 92, 93, and earlier and later versions of the Edge browser. Warning
19 users would have chilled engagement on Versions 90, 92, 93, and earlier and later versions of the
20 Edge browser as well as discouraged potential new users, and thus chilled use of Versions 90, 92,
21 93, and earlier and later versions of the Edge browser.

22 178. Defendant thus was not only able to evade or defer these costs, but it was able to
23 continue to accrue value and further benefit from the delay due to the time value of money.
24 Defendant has thus transferred all of the costs imposed by the unauthorized interception and
25 collection of users' private data described herein onto Plaintiffs and Class and Subclass members.
26 Defendant increased the cost to Plaintiffs and Class and Subclass members of mitigating the

1 interception and collection of their private data described herein by failing to notify them that
2 Defendant was intercepting and collecting Plaintiffs' and Class and Subclass members' private data
3 described herein.

4 179. In addition, Plaintiffs and Class and Subclass members have suffered from the
5 diminished value of their own private data described herein, which is property that has both personal
6 and economic value to Plaintiffs and Class and Subclass members.

7 180. Plaintiffs' and Class and Subclass members' private data described herein have
8 different forms of value. First, there is transactional, or barter, value. Indeed, Defendant has traded
9 (i) the ability to use Versions 90, 92, 93, and earlier and later versions of the Edge Browser in
10 exchange for (ii) the collection and use of Plaintiffs' and Class and Subclass members' private data
11 described herein—all while concealing the extent to which this information would be intercepted,
12 collected, and used.

13 181. Second, Plaintiffs' and Class and Subclass members' property, which has economic
14 value, was taken from them without their consent. There is a market for the private data described
15 herein, and it has at minimum a value greater than zero. Plaintiff and Class and Subclass members
16 cannot bring their private data described herein to market because Defendant's improper
17 interception, collection, and use of that private data for various reasons, including, but not limited
18 to, improving its software, services, and devices, providing targeted advertising, and developing its
19 sophisticated artificial intelligence and machine-learning systems means that Plaintiff's and Class
20 and Subclass members' private data described herein is no longer needed or marketable for that
21 purpose.

22 182. Third, in addition to the monetary value of selling their data, Plaintiff and Class and
23 Subclass members also assign value to keeping their private data described herein private. It is
24 possible to quantify this privacy value, which is destroyed when Defendant intercepts and collects
25 Plaintiffs' and Class and Subclass members' private data described herein without notice or
26 authorization.

183. Plaintiffs and Class and Subclass members were harmed when Defendant took their property and exerted exclusive control over it, intercepting and collecting it without Plaintiffs' and Class and Subclass members' knowledge to benefit Defendant and, additionally, for still undisclosed purposes.

184. Further, Defendant's control over these ever-expanding digital dossiers makes tracking and profiling Plaintiffs and Class and Subclass members, and targeting them with advertising, much more efficient and effective. Defendant unjustly earn substantial profits from such targeted advertising and/or from the sale of user data and/or information or services derived from such data.

185. In sum, Defendant has intercepted and collected Plaintiffs' and Class and Subclass members' private data described herein without providing anything of value to Plaintiffs and Class and Subclass members in exchange for that private data. Moreover, Defendant's unauthorized access to Plaintiffs' and Class and Subclass members' private data described herein has diminished the value of that private data. These actions and omissions by Defendant have resulted in harm to Plaintiffs and Class and Subclass members.

L. Microsoft Intercepted, Collected, and Used Plaintiffs' Private Data

186. Defendant's unauthorized interception, collection, and use of Plaintiffs' private data described herein resulted in the diminished value of that private content.

187. Plaintiff Saeedy has consistently used Edge since at least June of 2021 for both personal and work purposes as described in Paragraphs 7-10 . By associating the collected data with Saeedy's unique user identifiers and cookies, Defendant was and is able to determine his precise internet browsing activities and habits. Defendant thus utilized and configured the SmartScreen and Bing servers to transmit Plaintiff Saeedy's personally identifiable information without his express or implied consent.

188. Plaintiff Shah has consistently used Edge since at least June of 2021 on a computer provided by an employer or workplace as described in Paragraphs 11-14. By associating the

1 collected data with Shah's unique user identifiers and cookies, Defendant was and is able to
 2 determine his precise internet browsing activities and habits. Defendant thus utilized and configured
 3 the SmartScreen and Bing servers to transmit Plaintiff Shah's personally identifiable information
 4 without his express or implied consent.

5 189. Plaintiff Wilkinson has consistently used Edge since at least June of 2021 on a
 6 computer provided by an academic institution as described in Paragraphs 15-19. By associating the
 7 collected data with Wilkinson's unique user identifiers and cookies, Defendant was and is able to
 8 determine her precise internet browsing activities and habits. Defendant thus utilized and
 9 configured the SmartScreen and Bing servers to transmit Plaintiff Wilkinson's personally
 10 identifiable information without her express or implied consent.

11 190. Minor Plaintiff M.C. has consistently used Edge since at least 2020 for personal,
 12 educational, and medical purposes as described in Paragraphs 20-24. By associating the collected
 13 data with M.C.'s unique user identifiers and cookies, Defendant was and is able to determine M.C.'s
 14 precise internet browsing activities and habits. Defendant thus utilized and configured the
 15 SmartScreen and Bing servers to transmit Plaintiff M.C.'s personally identifiable information
 16 without M.C.'s express or implied consent.

17 **V. TOLLING, CONCEALMENT, AND ESTOPPEL**

18 191. Any applicable statutes of limitations have been tolled under (1) the fraudulent
 19 concealment doctrine, based on Defendant's knowing and active concealment and denial of the
 20 conduct alleged herein and (2) the delayed discovery doctrine, as Plaintiffs and Class and Subclass
 21 members did not and could not reasonably have discovered Defendant's conduct alleged herein until
 22 shortly before the Complaint was filed.

23 192. Defendant did not adequately disclose that it would intercept, collect, and use their
 24 private data described herein when users' used the Edge browser generally or that Defendant would
 25 still intercept, collect, and use their private data described herein even when the user followed
 26 Defendant's instructions on how to browse privately using an "inPrivate" window.

193. Moreover, Defendant's labeling of the relevant products' "Private Mode" as a "InPrivate" window is, in and of itself, misleading absent clear disclosures about the ways in which Defendant intercepts, collects, and uses users' private data. Indeed, "private" is commonly defined and understood as "not known or intended to be known publicly: secret."³⁶ However, as alleged above, Microsoft Edge takes users' information even when they are browsing the internet with Edge's "InPrivate" window.

194. Plaintiffs and Class and Subclass members did not discover and could not reasonably have discovered, that Defendant was intercepting and using their data in the ways set forth in this Complaint until shortly before the lawsuit was filed .

195. Plaintiffs and Class and Subclass members exercised reasonable diligence to protect their data from interception. Indeed, that is precisely the reason why they used Defendant's "InPrivate" browsing window. Yet Plaintiffs did not and could not reasonably have discovered their claims until consulting with counsel shortly before the filing of this Complaint through the exercise of reasonable diligence.

196. Accordingly, Plaintiffs and the Class and Subclass members could not have reasonably discovered the truth about Defendant's practices until shortly before Plaintiffs commenced this class litigation.

197. Defendant is therefore estopped from relying on any statute of limitations.

VI. CLASS ALLEGATIONS

198. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rule of Civil Procedure on behalf of the following Class and Subclasses:

Nationwide Class (the "Class"): All persons residing in the United States who used Microsoft's Edge browser to browse, enter keyword searches, or visit URLs and whose communications, including personal information,

³⁶ *Private*, Merriam-Webster, <https://www.merriam-webster.com/dictionary/private#:~:text=%3A%20not%20known%20or%20intended%20to,withdr awn%20from%20company%20or%20observation> (last visited July 21, 2023).

1 online browsing activity, key word searches, or visited URLs, Defendant
2 intercepted, received, or collected from July 29, 2015 through the present
(the “Class Period”).

3 Nationwide Business Subclass: All persons residing in the United States
4 who used Microsoft’s Edge browser to browse, enter keyword searches,
5 or visit URLs via a device provided by an employer or workplace that
6 came with the Edge browser pre-downloaded and whose communications,
7 including personal information, online browsing activity, key word
8 searches, or visited URLs, Defendant intercepted, received, or collected
9 during the Class Period.

10 Nationwide Academic Subclass: All persons residing in the United States
11 who used Microsoft’s Edge browser to browse, enter keyword searches,
12 or visit URLs via a device provided by an academic institution that came
13 with the Edge browser pre-downloaded and whose communications,
14 including personal information, online browsing activity, key word
15 searches, or visited URLs, Defendant intercepted, received, or collected
16 during the Class Period.

17 Nationwide Shared Devices Subclass: All persons residing in the United
18 States who used Microsoft’s Edge browser to browse, enter keyword
19 searches, or visit URLs on a shared or public device that they personally
20 did not download the Edge browser onto and whose communications,
21 including personal information, online browsing activity, key word
22 searches, or visited URLs, Defendant intercepted, received, or collected
23 during the Class Period.

24 Nationwide Minor Subclass: All persons residing in the United States who,
25 while under 18 years of age, used Microsoft’s Edge browser to browse,
26 enter keyword searches, or visit URLs and whose communications,
including personal information, online browsing activity, key word
searches, or visited URLs, Defendant intercepted, received, or collected
during the Class Period.

California Class (the “California Class”): All persons residing in the State
of California who used Microsoft’s Edge browser to browse, enter
keyword searches, or visit URLs and whose communications, including
personal information, online browsing activity, key word searches, or
visited URLs, Defendant intercepted, received, or collected from during
the Class Period.

California Business Subclass: All persons residing in the State of
California who used Microsoft’s Edge browser to browse, enter keyword
searches, or visit URLs via a device provided by an employer or workplace

1 that came with the Edge browser pre-downloaded and whose
2 communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
received, or collected during the Class Period.

3
4 California Academic Subclass: All persons residing in the State of
5 California who used Microsoft's Edge browser to browse, enter keyword
6 searches, or visit URLs via a provided by an academic institution that came
7 with the Edge browser pre-downloaded and whose communications,
including personal information, online browsing activity, key word
searches, or visited URLs, Defendant intercepted, received, or collected
during the Class Period.

8
9 California Shared Devices Subclass: All persons residing in the State of
10 California who used Microsoft's Edge browser to browse, enter keyword
11 searches, or visit URLs on a shared or public device that they personally
12 did not download the Edge browser onto and whose communications,
including personal information, online browsing activity, key word
searches, or visited URLs, Defendant intercepted, received, or collected
during the Class Period.

13
14 California Minor Subclass: All persons residing in the State of California
15 who, while under 18 years of age, used Microsoft's Edge browser to
16 browse, enter keyword searches, or visit URLs and whose
communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
received, or collected during the Class Period.

17
18 Washington Class (the "Washington Class"): All persons residing in the
19 State of Washington who used Microsoft's Edge browser to browse, enter
20 keyword searches, or visit URLs and whose communications, including
personal information, online browsing activity, key word searches, or
visited URLs, Defendant intercepted, received, or collected during the
Class Period.

21
22 Washington Business Subclass: All persons residing in the State of
23 Washington who used Microsoft's Edge browser to browse, enter keyword
24 searches, or visit URLs via a device provided by an employer or workplace
that came with the Edge browser pre-downloaded and whose
communications, including personal information, online browsing
activity, key word searches, or visited URLs, Defendant intercepted,
received, or collected during the Class Period.

25
26 Washington Academic Subclass: All persons residing in the State of
Washington who used Microsoft's Edge browser to browse, enter keyword

searches, or visit URLs via a device provided by an academic institution that came with the Edge browser pre-downloaded and whose communications, including personal information, online browsing activity, key word searches, or visited URLs, Defendant intercepted, received, or collected during the Class Period.

Washington Shared Devices Subclass: All persons residing in the State of Washington who used Microsoft's Edge browser to browse, enter keyword searches, or visit URLs on a shared or public device that they personally did not download the Edge browser onto and whose communications, including personal information, online browsing activity, key word searches, or visited URLs, Defendant intercepted, received, or collected during the Class Period.

Washington Minor Subclass: All persons residing in the State of Washington who, while under 18 years of age, used Microsoft's Edge browser to browse, enter keyword searches, or visit URLs and whose communications, including personal information, online browsing activity, key word searches, or visited URLs, Defendant intercepted, received, or collected during the Class Period.

199. Excluded from the Classes and Subclasses are: (1) the Court (including any judge or magistrate presiding over this action and any members of their families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

200. **Numerosity**: The Class and Subclass members are so numerous that joinder of all members is impracticable. The precise number of Class and Subclass members is unknown to Plaintiffs at this time but is believed to consist of millions of individuals who can be identified through Defendant's records.

201. **Typicality**: Plaintiffs' claims are typical of the claims of the Class and Subclass members, who are similarly affected by Defendant's wrongful conduct in violation of the laws

1 complained of herein. The claims of Plaintiffs and the members of the Class and Subclasses arise
 2 from the same conduct by Defendant and are based on the same legal theories. Defendant acted or
 3 refused to act on grounds generally applicable to the Class and Subclasses, and Defendant's policies
 4 and practices challenged herein apply equally and uniformly to each Class and Subclass member,
 5 including Plaintiffs. Plaintiffs do not have any interest that is in conflict with the interests of the
 6 Class or Subclass members.

7 **202. Predominant Common Questions:** Common questions of law and fact exist as to
 8 all members of the Classes and Subclasses and predominate over any questions affecting solely
 9 individual members of the Classes and Subclasses. Common questions for the Classes and
 10 Subclasses include, but are not limited to, the following:

11 a. Whether Defendant represented that Class and Subclass members could
 12 control what communications of user information, browsing history and web activity data were
 13 intercepted, received, or collected by Defendant;

14 b. Whether Defendant gave the Class and Subclass members a reasonable
 15 expectation of privacy that their communications of user information, browsing history and web
 16 activity data were not being intercepted, received, or collected by Defendant when the Class or
 17 Subclass member was using a browser while in "Private Mode";

18 c. Whether Defendant in fact intercepted, received, or collected
 19 communications of user information, browsing history and web activity from Class and Subclass
 20 members when the Class and Subclass members were using a browser while in "Private Mode";

21 d. Whether Defendant's practice of intercepting, receiving, or collecting
 22 communications of user information, browsing history and web activity violated state and federal
 23 privacy laws;

24 e. Whether Defendant's practice of intercepting, receiving, or collecting
 25 communications of user information, browsing history and web activity violated state and federal
 26 anti-wiretapping laws;

1 f. Whether Defendant's practice of intercepting, receiving, or collecting
2 communications of user information, browsing history and web activity violated any other state and
3 federal tort laws;

4 g. Whether Plaintiffs, Class, and Subclass members are entitled to declaratory
5 and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

6 h. Whether Plaintiffs, Class, and Subclass members have sustained damages as
7 a result of Defendant's conduct and if so, what is the appropriate measure of damages or restitution.

8 203. **Adequate Representation:** Plaintiffs have and will continue to fairly and adequately
9 represent and protect the interests of the Classes and Subclasses. Plaintiffs have retained counsel
10 competent and experienced in complex litigation and class actions, including litigations to remedy
11 privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Classes and
12 Subclasses, and Defendant has no defenses unique to any plaintiff. Plaintiffs and their counsel are
13 committed to vigorously prosecuting this action on behalf of the members of the Classes and
14 Subclasses, and they have the resources to do so. Neither Plaintiffs nor their counsel have any
15 interest adverse to the interests of the other members of the Classes and Subclasses.

16 204. **Superiority:** A class action is superior to other available methods for the fair and
17 efficient adjudication of this controversy and joinder of all members of the Classes and Subclasses
18 is impracticable. This proposed class action presents fewer management difficulties than individual
19 litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive
20 supervision by a single, able court. Class treatment will create economies of time, effort, and
21 expense and promote uniform decision-making. A class action is a particularly efficient and
22 appropriate procedure in this case because absent a class action Defendant would gain an
23 unconscionable economic advantage. Individual plaintiffs have limited resources and could be
24 outspent many times over by Defendant. Moreover, the recovery in each individual suit would not
25 cover the cost of litigation. Additionally, Defendant's course of conduct described herein is
26 common to each Class and Subclass member; maintaining individual actions would create a risk of

1 inconsistent results.

2 205. Plaintiffs reserve the right to revise the foregoing class allegations and definitions
3 based on facts learned and legal developments following additional investigation, discovery, or
4 otherwise.

5 **VII. CHOICE OF LAW**

6 206. California substantive law applies to every member of the California Class and
7 California Subclasses. California substantive law may be constitutionally applied to the claims of
8 the California Plaintiffs, California Class, and California Subclasses under the Due Process Clause,
9 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution.
10 California has significant contact, or significant aggregation of contacts, to the claims asserted by
11 the California Plaintiffs and California Class and California Subclasses members, thereby creating
12 state interests to ensure that the choice of California state law is not arbitrary or unfair.

13 207. Defendant conducts substantial business in California and has servers in California,
14 such that California has an interest in regulating Defendant's conduct under its laws. Defendant's
15 decision to conduct substantial business in California and avail itself of California's laws, renders
16 the application of California law to the claims herein constitutionally permissible.

17 208. The application of California law to the California Class and California Subclasses
18 is also appropriate under California and Washington's choice of law rules because California has
19 significant contacts to the claims of the California Plaintiffs and the proposed California Class and
20 California Subclasses, and California has a greater interest in applying its laws here than any other
21 interested state.

22 **FIRST CAUSE OF ACTION**

23 **(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*)**

24 **(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)**

25 209. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all
26 preceding paragraphs as if fully set forth herein.

1 210. Plaintiffs, the Classes, and Subclasses' private data described herein that Defendant
2 intercepted, collected, and used includes contents of electronic communications that Plaintiffs, the
3 Classes, and Subclasses intended to convey to recipients.

4 211. Plaintiffs, the Classes, and Subclasses had a reasonable expectation of privacy in their
5 private data described herein as well as in the collection and processing of their unique user
6 identifiers and cookies in connection with that content.

7 212. However, Defendant intentionally intercepted, collected, and used the private data
8 described herein contained in communications and messages transmitted via the Microsoft Edge
9 browser, and collected and processed users' unique user identifiers and cookies in connection with
10 that data, without Plaintiffs', the Classes', or Subclasses' consent or knowledge.

11 213. Defendant owned and operated the Microsoft Edge browser. Defendant collected
12 and intercepted Plaintiffs', the Classes', and Subclasses' private data described herein through
13 Versions 90, 92, 93, and earlier and later versions of Edge. Defendant transmitted this data to the
14 SmartScreen and/or Bing servers. Defendant used that data for various purposes, including, but not
15 limited to, improving its software, services, and devices, providing targeted advertising, and
16 developing its sophisticated artificial intelligence and machine-learning systems.

17 214. By associating the collected data with the unique user identifiers and cookies,
18 Defendant can and does determine individual users' precise internet browsing activities and habits.
19 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of
20 the Edge browser to collect and process users' unique user identifiers and cookies for this purpose.

21 215. Defendant was actively involved in designing and programming the data flows for
22 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
23 interception and collection alleged herein, and promoted the use of the Edge browser to California,
24 Washington, and U.S. residents, knowing about the privacy violations alleged herein.

25 216. The unauthorized interceptions described herein are not covered by any business
26 exception because the interceptions were not required to facilitate users' use of Versions 90, 92, 93,

1 and earlier and later versions of the Edge browser.

2 217. Plaintiffs, the Classes, and Subclasses could not provide consent to Defendant's
3 interception because they did not know that their private content was being intercepted and
4 reasonably anticipated that their private data described herein would remain private.

5 218. These acts violate § 2511(1)(a) of the Electronic Communications Privacy Act
6 ("ECPA") because Defendant intentionally endeavors to intercept, and does in fact intercept,
7 electronic content transmitted by Plaintiffs', the Classes', and Subclasses' use of Versions 90, 92,
8 93, and earlier and later versions of the Edge browser.

9 219. Defendant intercepts Plaintiffs', the Classes', and Subclasses' private data described
10 herein using the Microsoft Edge browser by collecting and sending that data to the SmartScreen
11 Server and/or Bing Servers along with users' unique user identifiers and cookies, by which
12 Defendant is able to determine individual users' precise browsing activities and habits.

13 220. Defendant's acts further violate § 2511(1)(d) because the information intercepted,
14 collected, and sent from Plaintiffs' and the Classes and Subclasses members' communications were
15 intentionally used for gain by Defendant as alleged above.

16 221. Plaintiffs, the Classes, and the Subclasses are also damaged when Defendant
17 intentionally intercepts, collects, and uses their information, despite knowing that such interception,
18 collection, and use was unauthorized, for corporate gain and profit such that Defendant was unjustly
19 enriched.

20 222. Plaintiffs, the Classes, and Subclasses seek: (i) injunctive relief to correct
21 Defendant's actions, including, but not limited to, requiring Defendant to stop intercepting,
22 collecting, or using any portion of, among other things, Plaintiffs', the Classes', and Subclasses'
23 private data described herein; (ii) the sum of actual damages suffered by them and any profits
24 Defendant made as a result of its violations of the ECPA, or statutory damages of whichever is the
25 greater of \$100 a day for each day of violation or \$10,000; and (iii) reasonable attorneys' fees and
26 costs under 18 U.S.C. § 2520.

SECOND CAUSE OF ACTION

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)

223. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

224. Plaintiffs', the Classes', and Subclasses' devices used to operate Versions 90, 92, and 93, and earlier and later versions of Edge are, and at all relevant times were, used for interstate communication and commerce and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B). Plaintiffs', the Classes', and Subclasses' internet browsing activity, which Defendant impermissibly tracked, involved submissions to websites for companies all over the United States, both for purchases of goods and information.

225. Defendant intentionally accessed Plaintiffs', the Classes', and Subclasses' protected computers and obtained information thereby, and in doing so exceeded authority granted by Plaintiffs, the Classes, and Subclasses to access the protected computers in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C). Plaintiffs, the Classes, and Subclasses have a civil cause of action for violation of the Computer Fraud and Abuse Act ("CFAA") under 18 U.S.C. § 1030(g) and have suffered damage or loss as follows.

226. Defendant's violations of the CFAA were intentional and reckless, or, pleaded in the alternative, negligent.

227. Defendant owned and operated the Microsoft Edge browser. Defendant intercepted and collected Plaintiffs', the Classes', and Subclasses' private data described herein along with their unique user identifiers and cookies through Versions 90, 92, 93, and earlier and later versions of Edge. Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data for various purposes, including, but not limited to, improving its software, services, and devices, providing targeted advertising, and developing its sophisticated artificial intelligence and machine-learning systems.

228. By associating the collected data with the unique user identifiers and cookies, Defendant can and does determine individual users' precise internet browsing activities and habits. Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of the Edge browser to collect and process users' unique user identifiers and cookies for this purpose.

229. Defendant was actively involved in designing and programming the data flows for Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful interception and collection alleged herein, and promoted the use of the Edge browser to California, Washington, and U.S. residents, knowing about the privacy violations alleged herein. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the unauthorized access to, collection, and use of Plaintiffs', the Classes', and Subclasses' private data described herein and the diminution in the value of that data, both of which occurred to millions of Class and Subclass members, easily aggregating at least \$5,000 in value during any of the 1-year periods at issue.

230. For these reasons, and those discussed in this Complaint, Plaintiffs, the Classes, and Subclasses are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

THIRD CAUSE OF ACTION

(Intrusion Upon Seclusion)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

231. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

232. California follows the Restatement (2nd) of Torts approach to liability for intrusion upon seclusion. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion

1 of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement (2nd)
2 of Torts § 652B.

3 233. A claim for intrusion upon seclusion requires (1) intrusion into a private place,
4 conversation, or matter; (2) in a manner highly offensive to a reasonable person.

5 234. The California Plaintiffs, California Class, and California Subclasses had a
6 reasonable expectation of privacy in their private data described herein as well as in the collection
7 and processing of their unique user identifiers in connection with that data.

8 235. The California Plaintiffs, California Class, and California Subclasses reasonably
9 expected that their private data described herein would not be collected, intercepted, and used by
10 Defendant. It is not necessary for the operation of Versions 90, 92, 93, and earlier and later versions
11 of the Edge browser for users’ private data described herein to be collected and intercepted by
12 Defendant. Furthermore, the California Plaintiffs, California Class, and California Subclasses were
13 not adequately notified that their private data described herein and unique user identifiers and cookies
14 would be intercepted, collected, processed, and used by Defendant.

15 236. Defendant intentionally intruded—and continues to intrude—upon the California
16 Plaintiffs’, California Class’s, and California Subclasses’ solitude, seclusion, and private affairs by
17 intentionally and secretly intercepting, collecting, and using the California Plaintiffs’, California
18 Class’s, and California Subclasses’ private data described herein and unique user identifiers and
19 cookies. Certain intrusions mentioned in this cause of action are illustrative and are not intended to
20 exclude from the scope of this cause of action all of the unlawful behavior as alleged against
21 Defendant herein.

22 237. Defendant owned and operated the Microsoft Edge browser. Defendant designed and
23 programmed Versions 90, 92, 93, and earlier and later versions of Edge to intercept, collect, and
24 send to Defendant the California Plaintiffs’, the California Class’s, and the California Subclasses’
25 private data described herein and unique user identifiers and cookies through Versions 90, 92, 93,
26 and earlier and later versions of Edge. Defendant transmitted this data to the SmartScreen and/or

1 Bing servers. Defendant used that data for various purposes, including, but not limited to, improving
2 its software, services, and devices, providing targeted advertising, and developing its sophisticated
3 artificial intelligence and machine-learning systems.

4 238. By associating the collected data with the unique user identifiers and cookies,
5 Defendant can and does determine individual users' precise internet browsing activities and habits.
6 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of
7 the Edge browser to collect and process users' unique user identifiers and cookies for this purpose.

8 239. Defendant was actively involved in designing, programming, and implementing the
9 data flows for Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the
10 unlawful interception and collection alleged herein, and promoted the use of the Edge browser to
11 California residents, knowing about the privacy violations alleged herein.

12 240. Defendant's intrusions are highly offensive to a reasonable person, as evidenced by
13 substantial research, literature, and governmental enforcement and investigative efforts to protect
14 consumer privacy against surreptitious technological intrusions. The intentionality of Defendant's
15 conduct, and the steps Defendant has taken to disguise it also reveals the highly offensive nature of its
16 conduct.

17 241. Defendant intercepted, collected, processed, and used the California Plaintiffs',
18 California Class's, and California Subclasses' private data described herein and unique user
19 identifiers and cookies without authority or consent from those California Plaintiffs, California Class
20 members, and California Subclass members.

21 242. The California Plaintiffs, California Class, and California Subclasses were all
22 harmed by, and continue to suffer harm as a direct and proximate result of Defendant's intrusions as
23 detailed throughout this Complaint and are entitled to just compensation and injunctive relief, as
24 well as such other relief as the Court may deem just and proper.

25 243. Defendant's conduct was a substantial factor in causing the harm suffered by the
26 California Plaintiffs, California Class, and California Subclasses.

244. The California Plaintiffs, California Class, and California Subclasses seek nominal and punitive damages as a result of Defendant's actions. Punitive damages are warranted because Defendant's malicious, oppressive, and willful actions were calculated to injure the California Plaintiffs, California Class, and California Subclasses, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in future misconduct.

245. The California Plaintiffs, California Class, and California Subclasses seek injunctive relief to remedy Defendant's actions, including, but not limited to, requiring Defendant to stop taking users' private and personally-identifiable data described herein; to make clear disclosures of the information that is reasonably necessary to operate the Microsoft Edge browser; and to recall and destroy all information already taken in contravention of the California Plaintiffs', California Class's, and California Subclasses' privacy rights.

246. The California Plaintiffs, California Class, and California Subclasses seek restitution and disgorgement for Defendant's intrusion upon seclusion. A person acting in conscious disregard of the rights of another must disgorge all profits because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CAUSE OF ACTION

(Violation of the Right to Privacy – California Constitution)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

247. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

248. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, Section 1 of its Constitution, which expressly provides that "[a]ll people are by

1 nature free and independent and have inalienable rights. Among these are enjoying and defending
 2 life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety,
 3 happiness, and privacy.” Cal. Const., art. I, § 1.

4 249. The right to privacy was added to the California Constitution after voters approved
 5 a legislative constitutional amendment designated as Proposition 11. Critically, the argument in
 6 favor of Proposition 11 reveals that the legislative intent was to curb businesses’ control over the
 7 unauthorized collection and use of consumers’ personal information, stating:

8 The right to privacy is the right to be left alone . . . It prevents
 9 government and business interests from collecting and stockpiling
 10 unnecessary information about us and from misusing information
 11 gathered for one purpose in order to serve other purposes or to
 12 embarrass us. Fundamental to our privacy is the ability to control
 circulating of personal information. This is essential to social
 relationships and personal freedom.³⁷

13 250. The principal purpose of this Constitutional right was to protect against unnecessary
 14 information gathering, use, and dissemination by public and private entities, including Defendant.

15 251. The right to privacy in California’s Constitution creates a private right of action
 16 against entities like Defendant.

17 252. To plead invasion of privacy under the California Constitution, the California
 18 Plaintiffs, California Class, and California Subclasses must allege “that (1) they possess a legally
 19 protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the
 20 intrusion is ‘so serious . . . as to constitute an egregious breach of the social norms’ such that the
 21 breach is ‘highly offensive.’” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th
 22 Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)).

23 253. The California Plaintiffs, California Class, and California Subclasses hold a legally
 24 protected privacy interest in their private and personally-identifiable data described herein that

25 ³⁷ BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH
 26 ARGUMENTS TO VOTERS, GEN. ELECTION *26 (NOV. 7, 1972).

1 Defendant intercepts, collects, and uses.

2 254. The California Plaintiffs, California Class, and California Subclasses have a legally
3 protected privacy interest in (a) precluding the interception, collection, copying, dissemination
4 and/or misuse of their private data described herein; and (b) making personal decisions and/or
5 conducting personal activities without observation, intrusion or interference, including, but not
6 limited to, the right to use Versions 90, 92, and 93, and earlier and later versions of the Edge browser,
7 and to visit and interact with various internet sites without having that information intercepted and
8 transmitted to Defendant without the knowledge or consent of the California Plaintiffs, California
9 Class, and California Subclasses.

10 255. The California Plaintiffs, California Class, and California Subclasses have a
11 reasonable expectation of privacy in the private data described herein that Defendant intercepts,
12 collects, and uses without adequate notice or consent – especially since it is not necessary for the
13 operation of the Edge browser for users’ private data described herein to be intercepted, collected,
14 processed, and used by Defendant.

15 256. Defendant’s actions constitute a serious invasion of privacy in that it: (a) invades a
16 zone of privacy protected by the Fourth Amendment, namely, the right to privacy in data contained
17 on personal computing devices, including web search and browsing histories; (b) violates federal
18 criminal laws including the Electronic Communications Privacy Act and Computer Fraud and
19 Abuse Act; and (c) invades the privacy interests and rights of millions of U.S. residents (including
20 the California Plaintiffs, California Class, and California Subclasses) without their consent.

21 257. Defendant fails to effectively inform users that Microsoft Edge intercepts, collects,
22 and uses private data. Defendant does not ensure that relevant disclosures are immediately apparent
23 and fails to disclose the extent of the information intercepted, received, or collected, or the result of
24 information that is intercepted, received, or collected. This results in injury to the California
25 Plaintiffs, California Class, and California Subclasses.

26 258. Defendant owned and operated the Microsoft Edge browser. Defendant collected and

1 intercepted the California Plaintiffs', California Class's, and California Subclasses' private data
2 described herein along with their unique user identifiers and cookies through Versions 90, 92, 93,
3 and earlier and later versions of Edge. Defendant transmitted this private data to the SmartScreen
4 and/or Bing servers. Defendant used that private data for various purposes, including, but not
5 limited to, improving its software, services, and devices, providing targeted advertising, and
6 developing its sophisticated artificial intelligence and machine-learning systems.

7 259. By associating the collected data with the unique user identifiers and cookies,
8 Defendant is able to and does determine individual users' precise internet browsing activities and
9 habits. Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later
10 versions of the Edge browser to collect and process users' unique user identifiers and cookies for
11 this purpose.

12 260. Defendant was actively involved in designing and programming the data flows for
13 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
14 interception and collection alleged herein, and promoted the use of the Microsoft Edge browser to
15 California residents, knowing about the privacy violations alleged herein.

16 261. Defendant acted with deceit and disregard for the California Plaintiffs', California
17 Class's, and California Subclasses' privacy by intercepting, collecting, and using private data described
18 herein without authorization.

19 262. The reasonableness of the California Plaintiffs', California Class's, and California
20 Subclasses' expectations of privacy is supported by the clandestine nature of Defendant's
21 interception and collection of the California Plaintiffs', California Class's, and California
22 Subclasses' private data described herein. Defendant acted with deceit and disregard for the
23 California Plaintiffs', California Class's, and California Subclasses' privacy.

24 263. Defendant's conduct violated the California Plaintiffs', California Class's, and
25 California Subclasses' privacy interests, was highly offensive to a reasonable person, and constituted
26 and continues to constitute an egregious breach of social norms. Not only did Defendant intercept,

1 collect, and use this private information, Defendant either did not disclose at all, or failed to make
2 an effective disclosure, that it would intercept, collect, and use the California Plaintiffs', California
3 Class's, and California Subclasses' private data described herein. Defendant intentionally invaded
4 the California Plaintiffs', California Class's, and California Subclasses' privacy interests by
5 intentionally designing its Edge browser to surreptitiously obtain, improperly gain knowledge of,
6 review, and retain the California Plaintiffs', California Class's, and California Subclasses' private
7 and personally-identifiable information.

8 264. These intrusions are highly offensive to a reasonable person, as evidenced by
9 substantial research, literature, and governmental enforcement and investigative efforts to protect
10 consumer privacy against surreptitious technological intrusions.

11 265. The intentionality of Defendant's conduct, and the steps it has taken to disguise it,
12 also show the highly offensive nature of its conduct.

13 266. Further, Defendant's conduct targeted the California Plaintiffs', California Class's,
14 and California Subclasses' computer devices, which the United States Supreme Court has
15 characterized as almost a feature of human anatomy, and which contain the California Plaintiffs',
16 California Class's, and California Subclasses' private and personally-identifiable information.

17 267. The California Plaintiffs, California Class, and California Subclasses were harmed
18 by the intrusion as detailed throughout this Complaint.

19 268. Defendant's conduct was a substantial factor in causing the harm suffered by the
20 California Plaintiffs, California Class, and California Subclasses.

21 269. The California Plaintiffs, California Class, and California Subclasses seek nominal
22 and punitive damages as a result of Defendant's actions. Punitive damages are warranted because
23 Defendant's malicious, oppressive, and willful actions were calculated to injure the California
24 Plaintiffs, California Class, and California Subclasses and were made in conscious disregard of their
25 rights. Punitive damages are also warranted to deter Defendant from engaging in future misconduct.

26 270. The California Plaintiffs, California Class, and California Subclasses seek injunctive

1 relief to remedy Defendant's actions, including, but not limited to, requiring Defendant to stop taking
 2 private information from users' electronic devices; to make clear disclosures of the information that
 3 is reasonably necessary to operate the Microsoft Edge browser; and to recall and destroy all private
 4 information already taken in contravention of the California Plaintiffs', California Class's, and
 5 California Subclasses' privacy rights.

6 271. The California Plaintiffs, California Class, and California Subclasses seek restitution
 7 and disgorgement for Defendant's violation of their privacy rights. A person acting in conscious
 8 disregard for the rights of another must disgorge all profit because disgorgement both benefits the
 9 injured parties and deters the perpetrator from committing the same unlawful actions again.
 10 Disgorgement is available for conduct that constitutes "conscious interference with a claimant's
 11 legally protected interests," including tortious conduct or conduct that violates another duty or
 12 prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

13 **FIFTH CAUSE OF ACTION**

14 **(Violation of California Invasion of Privacy Act, California Penal Code §§ 630, *et seq.*)**

15 **(California Plaintiffs, California Class, and California Subclasses**

16 **Against MICROSOFT CORP.)**

17 272. The California Plaintiffs, California Class, and California Subclasses repeat and
 18 incorporate by reference all preceding paragraphs as if fully set forth herein.

19 273. The California Invasion of Privacy Act ("CIPA"), codified at Cal. Pen. Code §§ 630-
 20 638, begins by providing its statement of purpose:

21 The Legislature hereby declares that advances in science and
 22 technology have led to the development of new devices and techniques
 23 for the purpose of eavesdropping upon private communications and that
 24 the invasion of privacy resulting from the continual and increasing use
 25 of such devices and techniques has created a serious threat to the free
 exercise of personal liberties and cannot be tolerated in a free and
 civilized society.

26 Cal. Pen. Code § 630.

1 274. Cal. Pen. Code § 631(a) imposes liability upon:

2 Any person who, by means of any machine, instrument, or contrivance,
3 or in any other manner . . . willfully and ***without the consent of all***
4 ***parties to the communication***, or in any unauthorized manner, reads, or
5 attempts to read, or to learn the contents or meaning of any message,
6 report, or communication while the same is in transit or passing over
7 any wire, line, or cable, or is being sent from, or received at any place
8 within this state; or who uses, or attempts to use, in any manner, or for
9 any purpose, or to communicate in any way, any information so
10 obtained, or who aids, agrees with, employs, or conspires with any
11 person or persons to lawfully do, or permit, or cause to be done any of
12 the acts or things mentioned above in this section [Emphasis
13 added.]

14 275. Cal. Pen. Code § 632(a) imposes liability upon:

15 A person who, intentionally and ***without the consent of all parties*** to a
16 confidential communication, uses an electronic amplifying or recording
17 device to eavesdrop upon or record the confidential communication,
18 whether the communication is carried on among the parties in the
19 presence of one another or by means of a telegraph, telephone, or other
20 device, except a radio [Emphasis added.]

21 276. Under either section of the CIPA quoted above, a defendant must show it had the
22 consent of all parties to a communication.

23 277. Defendant knowingly, willfully, and intentionally used and continues to use Versions
24 90, 92, 93, and earlier and later versions of the Edge browsers and receiving servers (where users'
25 private data described herein was and is saved and recorded), all of which are recording devices
26 under CIPA, to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic
27 communications containing the private data described herein from the California Plaintiffs,
28 California Class, and California Subclasses, while these electronic communications were and are in
29 transit, originating in or sent to California, and without the authorization or consent of the California
30 Plaintiffs, California Class, or California Subclasses.

31 278. The California Plaintiffs, California Class, and California Subclasses were and are in
32 California during one or more of the instances where Defendant intercepted their communications.

1 Upon information and belief, the California Plaintiffs, California Class, California Subclasses,
 2 during one or more of their interactions on the internet during the applicable statute of limitations
 3 period, communicated with one or more entities based in California, and/or with one or more entities
 4 whose servers were located in California. Communications from the California web-based entities
 5 to members of the California Class and California Subclasses were sent from California.
 6 Communications to the California web-based entities from members of the California Classes and
 7 California Subclasses were sent to California.

8 279. The communications intercepted by Defendant include “contents” of electronic
 9 communications exchanged between the California Plaintiffs, California Class, and California
 10 Subclasses, on the one hand, and the websites that they visited, on the other, in the form of the
 11 private data described herein. Defendant’s non-consensual interception of these communications
 12 was designed to learn at least some of these contents.

13 280. The following items constitute “machine[s], instrument[s], or contrivance[s]” under
 14 Cal. Penal Code § 631(a), and even if they did not, Defendant’s purposeful scheme that facilitated
 15 its interceptions falls under the broad statutory catch-all category of “any other manner”:

16 a. The California Plaintiffs’, California Class’s, and California Subclasses’
 17 browser (*i.e.*, the Edge Browser);

18 b. The California Plaintiffs’, California Class’s, and California Subclasses’
 19 personal computing devices;

20 c. The computer codes and programs used by Defendant to effectuate the
 21 interception of communications exchanged between websites and search engines, on the one hand,
 22 and the California Plaintiffs, California Class, and California Subclasses on the other;

23 d. Defendant’s servers, at least some of which, on information and belief, are
 24 located in California;

25 e. The servers of the third-party websites, at least some of which, on information
 26 and belief, are located in California, with respect to which Defendant intercepted the California

1 Plaintiffs', California Class's, and California Subclasses' communications;

2 f. The plan Defendant carried out to effectuate the interception of the
3 communications that were exchanged between the third-party websites, on the one hand, and the
4 California Plaintiffs, California Class, and California Subclasses on the other.

5 281. The private data described herein collected by Defendant constituted "confidential
6 communications," as that term is used in Cal. Pen. Code § 632(a), because the California Plaintiffs,
7 California Class, and California Subclasses have an objectively reasonable expectation of privacy
8 that their private browsing communications are not being intercepted, collected, disseminated, or
9 used by Defendant. In particular, it is not necessary for the operation of the Edge browser for users'
10 private data described herein to be intercepted, collected, disseminated, or used by Defendant.

11 282. The California Plaintiffs, California Class, and California Subclasses have suffered
12 loss because of these violations, including, but not limited to, violation of their rights to privacy and
13 loss of value in their private data described herein.

14 283. Pursuant to Cal. Pen. Code § 637.2, the California Plaintiffs, California Class, and
15 California Subclasses have been injured by the violations of Cal. Pen. Code §§ 631, 632, and each
16 seeks damages for the greater of \$5,000 or three times the amount of actual damages, as well as
17 injunctive or other equitable relief.

18 **SIXTH CAUSE OF ACTION**

19 **(Statutory Larceny, Cal. Penal Code §§ 484 and 496)**

20 **(California Plaintiffs, California Class, and California Subclasses**

21 **Against MICROSOFT CORP.)**

22 284. The California Plaintiffs, California Class, and California Subclasses repeat and
23 incorporate by reference all preceding paragraphs as if fully set forth herein.

24 285. Cal. Pen. Code § 496 imposes liability upon:

25 [e]very person who buys or receives any property that has been stolen
26 or that has been obtained in any manner constituting theft or extortion,
knowing the property to be so stolen or obtained, or who conceals, sells,

withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained[.]

286. Cal. Pen. Code § 484, which defines “theft”, states in pertinent part:

Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

287. Under California law, the California Plaintiff’s, California Class’s, and California Subclasses’ private data described herein constitutes property. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021). That property can be the subject of theft.

288. Defendant acted in a manner constituting theft by surreptitiously taking the California Plaintiffs’, California Class’s, and California Subclasses’ private data described herein through Version 90, 92, 93, and earlier and later versions of the Edge browser, with the specific intent to deprive those Plaintiffs and Class and Subclass members of their property.

289. Pursuant to Cal. Pen. Code § 496(c), the California Plaintiffs, California Class, and California Subclasses are entitled to treble damages, as well as attorneys’ fees and costs, for injuries sustained as a result of Defendant’s violations of Cal. Pen. Code § 496(a).

SEVENTH CAUSE OF ACTION

(Conversion)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

290. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

291. Conversion is the “wrongful exercise of dominion over the property of another.” *Culbertson-Stowers, Inc. v. Toyota Motor Credit Corp.*, 223 Cal.App.4th 202, 208 (2014).

292. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications. The California Plaintiffs', California Class's, and California Subclasses' private data as described herein is their property. *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021).

293. Defendant unlawfully intercepted, collected, used, and exercised dominion and control over the California Plaintiffs', California Class's, and California Subclasses' private data described herein without authorization.

294. Defendant wrongfully exercised control over the California Plaintiffs', California Class's, and California Subclasses' private data described herein and have not returned such data.

295. The California Plaintiffs, California Class, and California Subclasses have been damaged as a result of Defendant's unlawful conversion of their property.

EIGHTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*)

(California Plaintiffs, California Class, and California Subclasses

Against MICROSOFT CORP.)

296. The California Plaintiffs, California Class, and California Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

297. California's Unfair Competition Law ("UCL") prohibits any "unlawful unfair or fraudulent business act or practice." which can include false or misleading advertising. Cal. Bus. & Prof. Code §§ 17200 *et seq.*

298. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

299. Defendant engaged in "unlawful" conduct through its violation of state and federal law, including: (i) violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; (ii) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (iii) intrusion upon seclusion; (iv) invasion of privacy under Article I, Section 1 of the California Constitution; (v) violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; (vi) violation

1 of Cal. Penal Code §§ 484 and 496; and (vii) conversion.

2 300. Defendant engaged in “unfair” conduct, because it knowingly intercepted and
3 collected and used communications, and/or knowingly received intercepted communications,
4 containing the private data described herein of the California Plaintiffs and members of the
5 California Class and California Subclasses under circumstances in which those Plaintiffs and Class
6 and Subclasses members would have no reason to know that such information was being intercepted
7 and used because it was never disclosed or otherwise made known to them by Defendant. This
8 conduct offended established public policy established by the California legislature and is immoral,
9 unethical, oppressive, unscrupulous, and substantially injurious to consumers.

10 301. The California Plaintiffs, California Class, and California Subclasses have suffered
11 injury-in-fact, including the loss of money and/or property as a result of Defendant’s unfair and/or
12 unlawful practices, to wit, the unauthorized collection of their private data described herein, which
13 has value in an amount to be proven at trial. Moreover, the California Plaintiffs, California Class,
14 California Subclasses have suffered harm in the form of diminution of the value of their private data
15 described herein.

16 302. Defendant’s actions caused damage to and loss of the California Plaintiffs’,
17 California Class’s, and California Subclasses’ property right to control the dissemination and use of
18 their private data described herein.

19 303. Defendant has taken property from the California Plaintiffs, California Class, and
20 California Subclasses without providing just, or any, compensation.

21 304. Defendant should be required to cease their unfair and/or illegal collection of users’
22 private data described herein and to retrieve and delete all unfairly and/or illegally obtained private
23 user data. Defendant reaped unjust profits and revenues in violation of the UCL. The California
24 Plaintiffs, California Class, and California Subclasses seek injunctive relief governing Defendant’s
25 ongoing taking and possession of their private data described herein, and/or failure to account to the
26 California Plaintiffs, California Class, and California Subclasses concerning Defendant’s

1 interception, collection, possession, and use of that data, and restitution and disgorgement of
2 resulting unjust profits and revenues to Defendant.

3 305. The California Plaintiffs, California Class, and California Subclasses lack an
4 adequate remedy at law because the ongoing harms from Defendant's interception, collection,
5 taking, possession, and use of private data described herein must be addressed by injunctive relief
6 and, due to the ongoing and nature of the harm, the harm cannot be adequately addressed by
7 monetary damages alone.

8 **NINTH CAUSE OF ACTION**

9 **(Intrusion Upon Seclusion)**

10 **(Washington Plaintiff, Washington Class, and Washington Subclasses**

11 **Against MICROSOFT CORP.)**

12 306. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and
13 incorporate by reference all preceding paragraphs as if fully set forth herein.

14 307. Washington follows a common law cause of action for invasion of privacy by intrusion
15 upon seclusion. *Reid v. Pierce County*, 961 P.2d 333 (Wash. 1998). "Invasion of privacy by intrusion
16 consists of a deliberate intrusion, physical or otherwise, into a person's solitude, seclusion, or private
17 affairs. [To prevail on this cause of action] the intruder must have acted deliberately to achieve the
18 result, with the certain belief that the result would happen." *Fisher v. State Dep't of Health*, 106 P.3d
19 836, 879 (Wash. Ct. App. 2005).

20 308. The Washington Plaintiff, Washington Class, and Washington Subclasses had a
21 reasonable expectation of privacy in their private data described herein as well as in the collection
22 and processing of their unique user identifiers in connection with that content.

23 309. The Washington Plaintiff, Washington Class, and Washington Subclasses
24 reasonably expected that their private data described herein would not be collected, intercepted, and
25 used by the Defendant. It is not necessary for the operation of Versions 90, 92, 93, and earlier and
26 later versions of the Edge browser for such data to be collected, intercepted, and used by Defendant.

1 310. Defendant intentionally intruded—and continues to intrude—upon the Washington
 2 Plaintiff's, Washington Class's, and Washington Subclasses' solitude, seclusion, and private affairs
 3 by intentionally and secretly collecting the Washington Plaintiff's, Washington Class's,
 4 Washington Subclasses' private and personally-identifiable information and using that data, as
 5 described above. Certain intrusions are shared within this claim as illustrative; however, not to the
 6 exclusion of all of the unlawful behavior as alleged against Defendant herein.

7 311. Defendant owned and operated the Microsoft Edge browser. Defendant collected
 8 and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
 9 private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge.
 10 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
 11 for various purposes, including, but not limited to, improving its software, services, and devices,
 12 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
 13 learning systems. By associating the collected data with the unique user identifiers and cookies,
 14 Defendant is able to determine individual users' precise internet browsing activities and habits.
 15 Defendant thus designed and programmed Versions 90, 92, 93, and earlier and later versions of the
 16 Edge browser to collect and process users' unique user identifiers and cookies.

17 312. Defendant was actively involved in designing and programming the data flows for
 18 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
 19 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
 20 Washington and U.S. residents, knowing about the privacy violations alleged herein.

21 313. Defendant's intrusions are highly offensive to a reasonable person, as evidenced by
 22 substantial research, literature, and governmental enforcement and investigative efforts to protect
 23 consumer privacy against surreptitious technological intrusions. The intentionality of Defendant's
 24 conduct, and the steps it has taken to disguise it also reveals the highly offensive nature of its conduct.

25 314. Defendant collected, intercepted, processed, and used the Washington Plaintiff's,
 26 Washington Class's, and Washington Subclasses' private data described herein and unique user

1 identifiers and cookies without authority or consent from that Plaintiff and members of that Class and
2 those Subclasses.

3 315. The Washington Plaintiff, Washington Class, and Washington Subclasses were all
4 harmed by, and continue to suffer harm as a direct and proximate result of Defendant's intrusions,
5 as detailed throughout this Complaint, and are entitled to just compensation and injunctive relief, as
6 well as such other relief as the Court may deem just and proper.

7 316. Defendant's conduct was a substantial factor in causing the harm suffered by the
8 Washington Plaintiff, Washington Class, and Washington Subclasses.

9 317. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
10 nominal and punitive damages because of Defendant's actions. Punitive damages are warranted
11 because Defendant's malicious, oppressive, and willful actions were calculated to injure the
12 Washington Plaintiff, Washington Class, and Washington Subclasses, and were made in conscious
13 disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in
14 future misconduct.

15 318. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
16 injunctive relief to remedy Defendant's actions, including, but not limited to, requiring Defendant
17 to stop taking private and personally-identifiable information from users' electronic devices; to make
18 clear disclosures of the information that is reasonably necessary to operate the Microsoft Edge
19 browser; and to recall and destroy all information already taken in contravention of the Washington
20 Plaintiff's, Washington Class's, and Washington Subclasses' privacy rights.

21 **TENTH CAUSE OF ACTION**

22 **(Conversion)**

23 **(Washington Plaintiff, Washington Class, and Washington Subclasses**

24 **Against MICROSOFT CORP.)**

25 319. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and
26 incorporate by reference all preceding paragraphs as if fully set forth herein.

1 320. Conversion is the unjustified, willful interference with a chattel which deprives a
2 person entitled to the property of possession. “Chattel” includes both tangible and intangible goods,
3 such as corporate property. *Lang v. Hougan*, 136 Wn. App. 708, 718 (Wash. Ct. App. 2007). The
4 essence of conversion is the dispossession of property from the rightful owner. *Repin v. State*, 198
5 Wn. App. 243, 270 (Wash. Ct. App. 2017). The Washington Plaintiff, Washington Class, and
6 Washington Subclasses have a property interest in their personal information.

7 321. Defendant unlawfully collected, used, and exercised dominion and control over the
8 California Plaintiffs, Class, and Subclasses’ private data described herein without authorization.

9 322. Defendant owned and operated the Microsoft Edge browser. Defendant collected
10 and intercepted the Washington Plaintiff’s, Washington Class’s, and Washington Subclasses’
11 private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge.
12 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
13 for various purposes, including, but not limited to, improving its software, services, and devices,
14 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
15 learning systems.

16 323. By associating the collected data with the unique user identifiers and cookies,
17 Defendant is able to determine individual users’ precise internet browsing activities and habits.
18 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of
19 the Edge browser to collect and process users’ unique user identifiers and cookies.

20 324. Defendant wrongfully exercised control over the Washington Plaintiff’s,
21 Washington Class’s, and Washington Subclasses’ private data described herein and have not
22 returned it.

23 325. The Washington Plaintiff, Washington Class, and Washington Subclasses have been
24 damaged as a result of Defendant’s unlawful conversion of their private data described herein. The
25 reasonable and fair market value of the unlawfully obtained private data can be determined in the
26 marketplace.

ELEVENTH CAUSE OF ACTION

(Violation of the Washington Privacy Act, Wash. Rev. Code ch. 9.73)

(Washington Plaintiff, Washington Class, and Washington Subclasses

Against MICROSOFT CORP.)

326. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

327. Washington's Privacy Act ("WPA") prohibits the interception or recording of a private communication or conversation by any device, electronic or otherwise, without obtaining the consent of all the parties participating in the conversation. RCW § 9.73.030(1)(a)(b). Under the WPA, communication is private when parties "manifest a subjective intention that it be private and where that expectation is reasonable." *State v. Kipp*, 179 Wn.2d. 718, 729 (Wash. Ct. App. 2014). Proof of subjective intent need not be explicit. *Id.* at 729.

328. The Washington Plaintiff, Washington Class, and Washington Subclasses have an expectation of privacy in their private data described herein, and they exercised a reasonable expectation of privacy concerning the transmission of that content.

329. However, Defendant intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses' private data described herein without their consent or knowledge.

330. Defendant owned and operated the Microsoft Edge browser. Defendant collected and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses' private data described herein through Versions 90, 92, 93, and earlier and later versions of Edge. Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data for various purposes, including, but not limited to, improving its software, services, and devices, providing targeted advertising, and developing its sophisticated artificial intelligence and machine-learning systems.

331. By associating the collected data with the unique user identifiers and cookies, Defendant is able to determine individual users' precise internet browsing activities and habits.

1 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of
2 the Edge browser to collect and process users' unique user identifiers and cookies.

3 332. Defendant was actively involved in designing and programming the data flows for
4 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
5 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
6 Washington and U.S. residents, knowing about the privacy violations alleged herein.

7 333. Defendant designed the Microsoft Edge browser in a way that it knew the
8 Washington Plaintiff's, Washington Class's, and Washington Subclasses' privacy rights would be
9 violated, in that their content would be unlawfully intercepted. The defective and unlawful design
10 of the Microsoft Edge browser directly facilitates Defendant's unlawful conduct.

11 334. The unauthorized interceptions described herein are not covered by any business
12 exception because the interceptions were not required to facilitate communications between users.

13 335. The Washington Plaintiff, Washington Class, and Washington Subclasses could not
14 provide consent to the interception because they did not know that their private data described herein
15 was being intercepted and reasonably anticipated that such data would remain private.

16 336. The Washington Plaintiff, Washington Class, and Washington Subclasses have a
17 property right and interest in their private data described herein such that the interception of that
18 data is violative of those rights and therefore causes them injury and damages.

19 337. The Washington Plaintiff, Washington Class, and Washington Subclasses suffered
20 further economic injury as a result of Defendant's unlawful and unauthorized collection,
21 interception, and use of their private data described herein.

22 338. The Washington Plaintiff, Washington Class, and Washington Subclasses seek the
23 amount of their actual damages in the amount of \$100 for each day of violation not to exceed \$1,000,
24 liquidated damages, reasonable attorneys' fees and costs, and any other relief this court deems just.

TWELFH CAUSE OF ACTION

(Violation of the Washington Consumer Protection Act, Wash. Rev. Code ch. 19.86)

(Washington Plaintiff, Washington Class, and Washington Subclasses

Against MICROSOFT CORP.)

339. The Washington Plaintiff, Washington Class, and Washington Subclasses repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

340. The Washington Consumer Protection Act (“WCPA”) makes unlawful any unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. RCW § 19.86.020. “Trade or commerce” includes any commerce directly or indirectly affecting the people of the state of Washington. Wash. Rev. Code Ann § 19.86.010. An unfair or deceptive act is proved if the defendant’s actions possessed a tendency or capacity to mislead. *Testo v. Russ Dunmire Oldsmobile, Inc.*, 554 P.2d 349 (1976).

341. The Washington Plaintiff, Washington Class, and Washington Subclasses hold a legally protected privacy interest in their private data described herein that Defendant has unfairly collected, intercepted, and used through deceptive acts and practices.

342. The Washington Plaintiff, Washington Class, and Washington Subclasses had a reasonable expectation of privacy in their private data described herein as well as in the collection and processing of their unique user identifiers in connection with that content.

343. The Washington Plaintiff, Washington Class, and Washington Subclasses reasonably expected that their private data described herein would not be collected and intercepted by the Microsoft Edge browser. It is not necessary for the operation of the browser for users’ private data described herein to be collected, intercepted, and used by Defendant.

344. These unfair or deceptive acts or practices taken by Defendant include failing to inform the user that Edge collects and intercepts the user’s private data described herein, not ensuring relevant disclosures are immediately apparent, and failing to disclose the extent of the

1 information collected, intercepted, or used, or the result of information that is collected, intercepted,
2 or used.

3 345. The Washington Plaintiff, Washington Class, and Washington Subclasses can claim
4 that these deceptive acts and practices are injurious to the public interest because they injure other
5 persons and have the capacity to injure other persons.

6 346. Defendant owned and operated the Microsoft Edge browser. Defendant collected
7 and intercepted the Washington Plaintiff's, Washington Class's, and Washington Subclasses'
8 private data described herein through Versions 90, 92, 93 and earlier and later versions of Edge.
9 Defendant transmitted this data to the SmartScreen and/or Bing servers. Defendant used that data
10 for various purposes, including, but not limited to, improving its software, services, and devices,
11 providing targeted advertising, and developing its sophisticated artificial intelligence and machine-
12 learning systems.

13 347. By associating the collected data with the unique user identifiers and cookies,
14 Defendant is able to determine individual users' precise internet browsing activities and habits.
15 Defendant thus designed and programmed Versions 90, 92, and 93, and earlier and later versions of
16 the Edge browser to collect and process users' unique user identifiers and cookies.

17 348. Defendant was actively involved in designing and programming the data flows for
18 Versions 90, 92, 93, and earlier and later versions of the Edge browser, including the unlawful
19 collection interception alleged herein, and promoted the use of the Microsoft Edge browser to
20 California and U.S. residents, knowing about the privacy violations alleged herein.

21 349. Defendant acted with deceit and disregard for the Washington Plaintiff's, Washington
22 Class's, and Washington Subclasses' privacy by collecting, intercepting, and using their private data
23 described herein without authorization.

24 350. Defendant's conduct violated the Washington Plaintiff's, Washington Class's, and
25 Washington Subclasses' privacy interests, were highly offensive to a reasonable person, and
26 constituted and continues to constitute an egregious breach of social norms. Not only did Defendant

1 take and use this information, Defendant either did not disclose at all, or failed to make an effective
2 disclosure, that it would take and use the Washington Plaintiff's, Washington Class's, and
3 Washington Subclasses' private and personally-identifiable information. Defendant intentionally
4 invaded the Washington Plaintiff's, Washington Class's, and Washington Subclasses' privacy
5 interests by intentionally designing its Edge browser to surreptitiously obtain, improperly gain
6 knowledge of, review, and retain the Washington Plaintiff's, Washington Class's, and Washington
7 Subclasses' private data described herein.

8 351. These intrusions are highly offensive to a reasonable person, as evidenced by
9 substantial research, literature, and governmental enforcement and investigative efforts to protect
10 consumer privacy against surreptitious technological intrusions.

11 352. The intentionality of Defendant's conduct, and the steps it has taken to disguise it also
12 show the highly offensive nature of its conduct.

13 353. Further, Defendant's conduct targeted the Washington Plaintiff's, Washington
14 Class's, and Washington Subclasses' computer devices, which the United States Supreme Court has
15 characterized as almost a feature of human anatomy, and which contain the Washington Plaintiff's,
16 Washington Class's, and Washington Subclasses' private and personally-identifiable information.

17 354. The Washington Plaintiff, Washington Class, and Washington Subclasses were
18 harmed by the intrusion as detailed throughout this Complaint.

19 355. Defendant's conduct was a substantial factor in causing the harm suffered by the
20 Washington Plaintiff, Washington Class, and Washington Subclasses.

21 356. The Washington Plaintiff, Washington Class, and Washington Subclasses seek the
22 amount of their actual damages to not exceed more than \$7,500 for each violation, plus reasonable
23 attorneys' fees and costs, and any other relief this court deems just.

24 357. The Washington Plaintiff, Washington Class, and Washington Subclasses seek
25 nominal and punitive damages as a result of Defendant's actions. Punitive damages are warranted
26 because Defendant's malicious, oppressive, and willful actions were calculated to injure the

1 Washington Plaintiffs, Washington Class, and Washington Subclasses and were made in conscious
 2 disregard of their rights. Punitive damages are also warranted to deter Defendant from engaging in
 3 future misconduct.

4 358. The Washington Plaintiff, Washington Class, and Washington Subclasses seek injunctive
 5 relief to remedy Defendant's actions, including, but not limited to, requiring Defendant to stop taking
 6 private information from users' electronic devices; to make clear disclosures of the information that is
 7 reasonably necessary to operate the Microsoft Edge browser; and to recall and destroy all
 8 information already taken in contravention of the Washington Plaintiff's, Washington Class's, and
 9 Washington Subclasses' privacy rights.

10 **THIRTEENTH CAUSE OF ACTION**

11 **(Restitution / Unjust Enrichment)**

12 **(All Plaintiffs, Classes, and Subclasses Against MICROSOFT CORP.)**

13 359. Plaintiffs, the Classes, and Subclasses repeat and incorporate by reference all
 14 preceding paragraphs as if fully set forth herein.

15 360. Plaintiffs, the Classes, and Subclasses have conferred substantial benefits on
 16 Defendant by downloading and using Defendant's Edge browser. These benefits include
 17 Defendant's collection and use of the Plaintiffs', the Classes', and the Subclasses' private data
 18 described herein and the revenues and profits resulting from using this data for various purposes,
 19 including, but not limited to, those described herein.

20 361. Defendant has knowingly and willingly accepted and enjoyed these benefits.

21 362. Defendant either knew or should have known that the benefits rendered by Plaintiffs,
 22 the Classes, and Subclasses were given and received with the expectation that it would not take and
 23 use the private data described herein that Defendant has taken without permission. For Defendant
 24 to retain those benefits under these circumstances is inequitable.

1 G. Grant such other and further legal and equitable relief as the Court deems just and
2 equitable.

3 **DEMAND FOR JURY TRIAL**

4 Plaintiffs demand a trial by jury on all issues so triable.

5
6 DATED this 25th day of January 2024.

7 Respectfully submitted,

8 SUMMIT LAW GROUP, PLLC

9 By s/ Alexander A. Baehr

10 Alexander A. Baehr, WSBA No. 25320
11 315 Fifth Avenue S., Suite 1000
12 Seattle, Washington 98104
Telephone: (206) 676-7000
Email: alexb@summitlaw.com

13 BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
14 DROOKS, LINCENBERG & RHOW, PC

15 Ekwan E. Rhow (*pro hac vice forthcoming*)
16 Marc E. Masters (*pro hac vice forthcoming*)
17 Barr Benyamin (*pro hac vice forthcoming*)
18 1875 Century Park East, 23rd Floor
Los Angeles, California 90067
Telephone: (310) 201-2100
Email: erhow@birdmarella.com
mmasters@birdmarella.com
bbenyamin@birdmarella.com

19
20 GLANCY PRONGAY & MURRAY LLP

21 Jonathan Rotter (*pro hac vice forthcoming*)
22 Raymond D. Sulentic (*pro hac vice*
23 *forthcoming*)
24 1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: jrotter@glancylaw.com
rsulentic@glancylaw.com

CLARKSON LAW FIRM, P.C.

Glenn A. Danas (*pro hac vice forthcoming*)

Yana Hart (*pro hac vice forthcoming*)

Katelyn M. Leeviraphan (*pro hac vice
forthcoming*)

22525 Pacific Coast Highway

Malibu, CA 90265

Tel: (213) 788-4050

Fax: (213) 788-4070

Email: gdanas@clarksonlawfirm.com

yhart@clarksonlawfirm.com

kleeviraphan@clarksonlawfirm.com

Attorneys for Plaintiffs and
the Putative Classes and Subclasses